Model checking with Interval Temporal Logic: Results and Perspectives

Angelo Montanari

Dept. of Mathematics, Computer Science, and Physics
University of Udine, Italy

October 29, 2018

Model checking

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

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

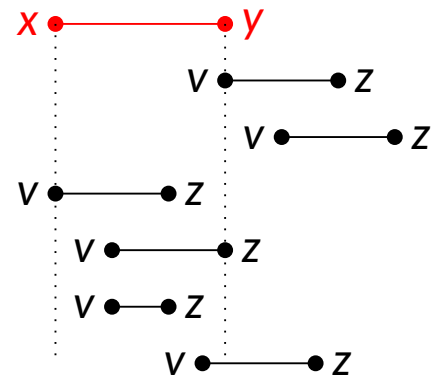
Point-based vs. interval-based MC

- MC 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, CTL, and CTL*.

- Interval-based MC:
  - interval-based properties express conditions on computation stretches
  - they are specified by means of interval temporal logics, which feature intervals as their basic ontological entities
    - » ability to express, for instance, actions with duration, accomplishments, aggregations
    - » applications in the areas of computational linguistics, artificial intelligence, temporal databases, formal verification, etc.

The logic HS

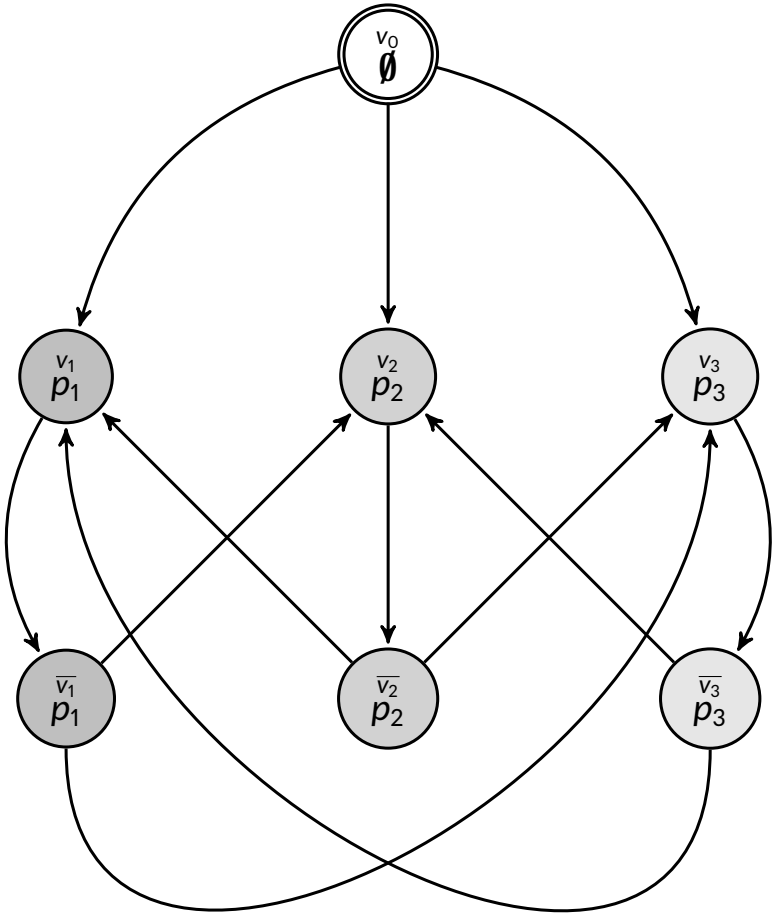
HS features a modality for each of the 13 Allen's ordering relations between pairs of intervals (except for equality)

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	$\langle O \rangle$	$[x,y]\mathcal{R}_O[v,z] \iff x < v < y < z$	

$$\psi ::= p \mid \neg\psi \mid \psi \vee \psi \mid \langle X \rangle \psi \mid \langle \overline{X} \rangle \psi \qquad X \in \{A, L, B, E, D, O\}.$$

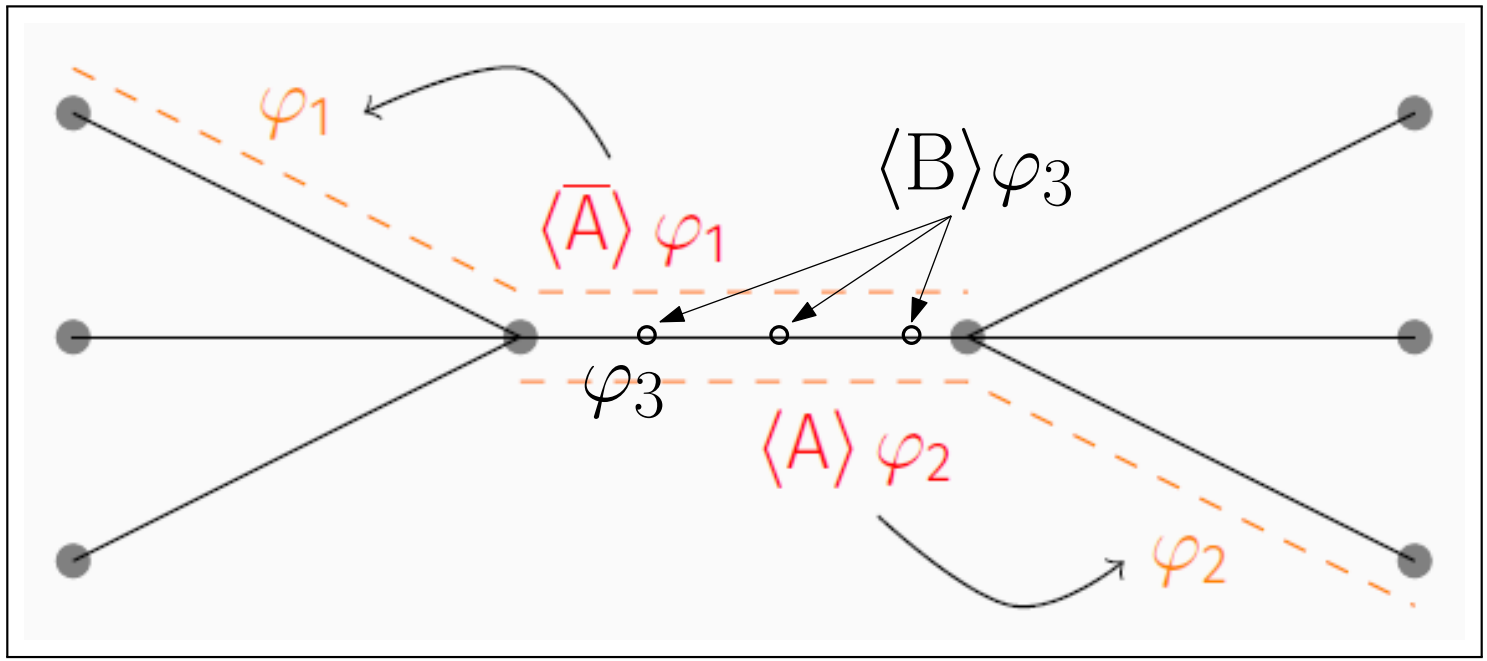
All modalities can be expressed by means of $\langle A \rangle$, $\langle B \rangle$, $\langle E \rangle$ and their transposed modalities $\langle \overline{A} \rangle$, $\langle \overline{B} \rangle$, $\langle \overline{E} \rangle$ only

Kripke structures



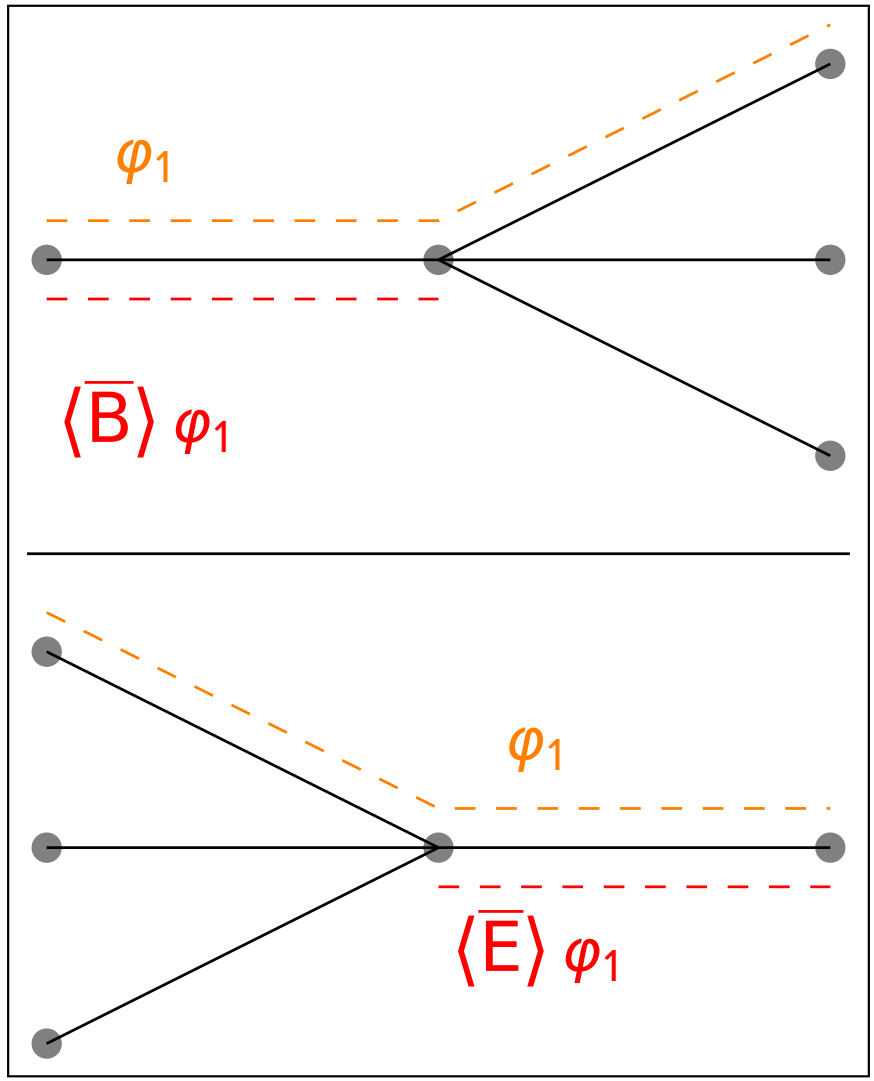
- HS formulas are interpreted over (finite) state-transition systems whose states are labeled with sets of proposition letters (Kripke structures)
- An interval is a trace (finite path) in a Kripke structure

HS (state-based) semantics



- Branching semantics of past/future operators

HS (state-based) semantics



- Branching semantics of past/future operators

HS (state-based) semantics and MC

Truth of a formula ψ over a trace ρ of a Kripke structure:

- ρ models $p \iff p$ labels all states of ρ, for any letter $p \in \mathcal{AP}$ (homogeneity assumption);

HS (state-based) semantics and MC

Truth of a formula ψ over a trace ρ of a Kripke structure:

- ρ models $p \iff p \in \mu(\mathsf{fst}(\rho), \mathsf{lst}(\rho))$, for any letter $p \in \mathcal{AP}$ (endpoint-based labeling);

HS (state-based) semantics and MC

Truth of a formula ψ over a trace ρ of a Kripke structure:

- ρ models $r \Leftrightarrow \mu(\rho) \in \mathscr{L}(r)$
  (labeling based on regular expressions, subsuming the others);

HS (state-based) semantics and MC

Truth of a formula ψ over a trace ρ of a Kripke structure:

- ρ models $r \Leftrightarrow \mu(\rho) \in \mathscr{L}(r)$
  (labeling based on regular expressions, subsuming the others);
- negation, disjunction, and conjunction are standard;
- $\mathcal{K}, \rho \models \langle \mathsf{A} \rangle \psi \ldots$;
- $\mathcal{K}, \rho \models \langle \mathsf{B} \rangle \psi \ldots$;
- $\mathcal{K}, \rho \models \langle \mathsf{E} \rangle \psi \ldots$;
- inverse operators $\langle \overline{\mathsf{A}} \rangle$, $\langle \overline{\mathsf{B}} \rangle$, $\langle \overline{\mathsf{E}} \rangle$

HS (state-based) semantics and MC

Truth of a formula ψ over a trace ρ of a Kripke structure:

- ρ models $r \Leftrightarrow \mu(\rho) \in \mathscr{L}(r)$
  (labeling based on regular expressions, subsuming the others);
- negation, disjunction, and conjunction are standard;
- $\mathcal{K}, \rho \models \langle \mathsf{A} \rangle \psi \ldots$;
- $\mathcal{K}, \rho \models \langle \mathsf{B} \rangle \psi \ldots$;
- $\mathcal{K}, \rho \models \langle \mathsf{E} \rangle \psi \ldots$;
- inverse operators $\langle \overline{\mathsf{A}} \rangle$, $\langle \overline{\mathsf{B}} \rangle$, $\langle \overline{\mathsf{E}} \rangle$

MC

$\mathcal{K} \models \psi \iff$ all *initial* traces of $\mathcal{K}$ model ψ

Possibly infinitely many traces!

MC: the key notion of BE_k-descriptor

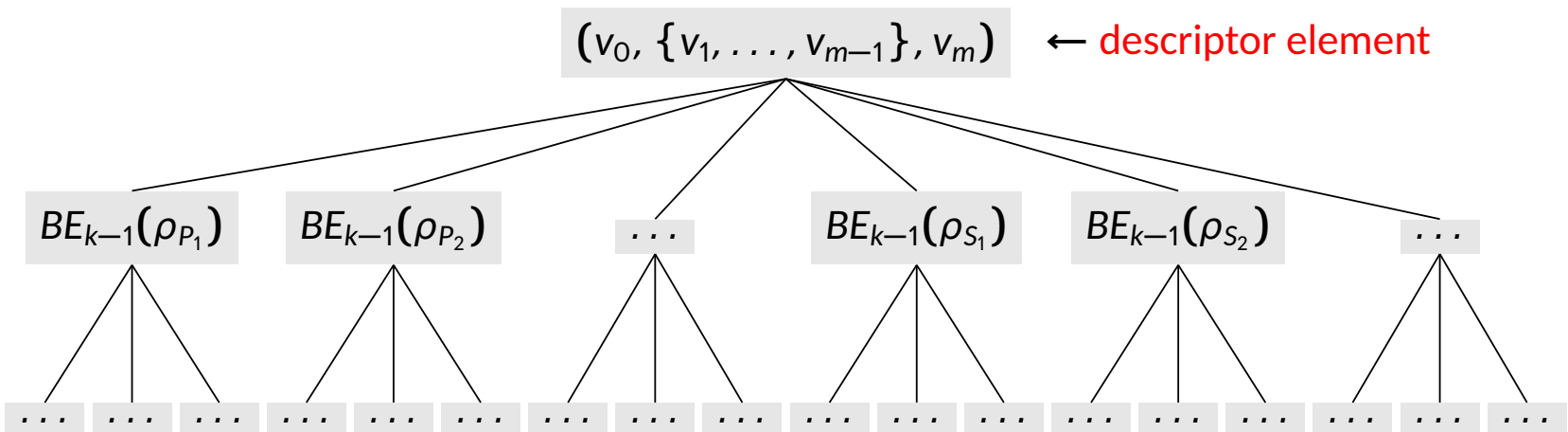
- The BE-nesting depth of an HS formula ψ ($\mathtt{Nest}_{\mathsf{BE}}(\psi)$) is the maximum degree of nesting of modalities B and E in ψ
- Two traces ρ and ρ' of a Kripke structure $\mathcal{K}$ are k-equivalent iff:
  $\mathcal{K}, \rho \models \psi$ iff $\mathcal{K}, \rho' \models \psi$ for all HS formulas ψ with $\mathtt{Nest}_{\mathsf{BE}}(\psi) \leq k$

MC: the key notion of BE_k-descriptor

- The BE-nesting depth of an HS formula ψ ($\mathtt{Nest}_{\mathtt{BE}}(\psi)$) is the maximum degree of nesting of modalities B and E in ψ
- Two traces ρ and ρ' of a Kripke structure $\mathcal{K}$ are k-equivalent iff:

  $\mathcal{K}, \rho \models \psi$ iff $\mathcal{K}, \rho' \models \psi$ for all HS formulas ψ with $\mathtt{Nest}_{\mathtt{BE}}(\psi) \leq k$

For any given k, we provide a suitable tree representation for a trace, called a BE_k-descriptor: the BE_k-descriptor $BE_k(\rho)$ for a trace $\rho = v_0 v_1 \ldots v_{m-1}\, v_m$ has the following structure:

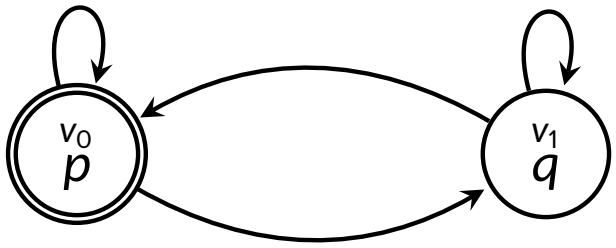


↑ $\rho_{P_1}, \rho_{P_2}, \ldots$ prefixes of ρ

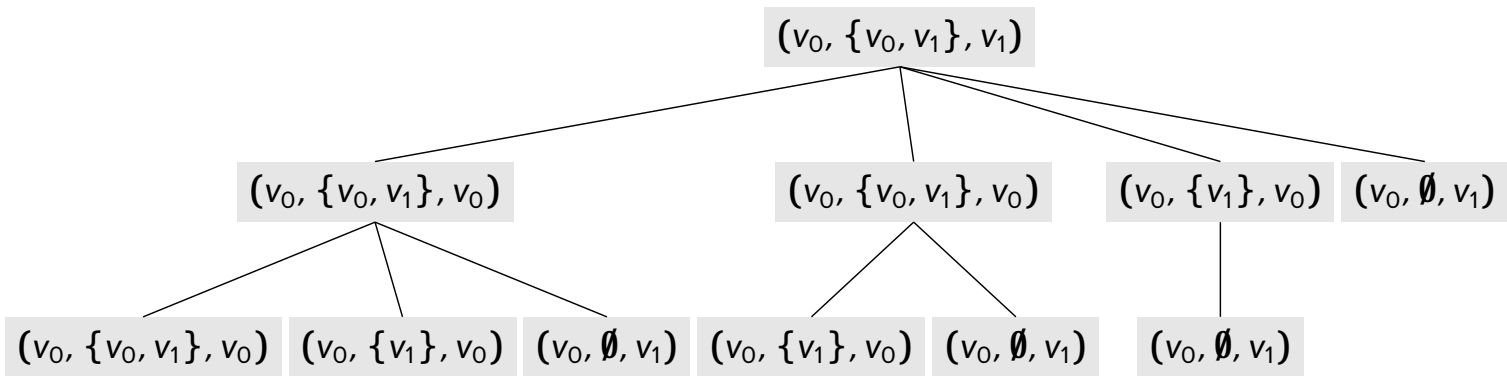
↑ $\rho_{S_1}, \rho_{S_2}, \ldots$ suffixes of ρ

Remark: the descriptor does not feature sibling isomorphic subtrees

An example of a BE_2-descriptor



The BE_2-descriptor for the trace $\rho = v_0 v_1 v_0^4 v_1$ (for the sake of readability, only the subtrees for prefixes are displayed and point intervals are excluded)



Remark: the subtree to the left is associated with both prefixes $v_0 v_1 v_0^3$ and $v_0 v_1 v_0^4$ (no sibling isomorphic subtrees in the descriptor)

Two basic facts

FACT 1

For any Kripke structure $\mathcal{K}$ and any BE-nesting depth $k \geq 0$, the number of different BE_k-descriptors is finite (and thus at least one descriptor has to be associated with infinitely many traces)

FACT 2

Two traces ρ and ρ' of a Kripke structure $\mathcal{K}$ described by the same BE_k-descriptor are k-equivalent

Decidability of the MC problem for HS

Theorem

The MC problem for full HS *over Kripke structures, under homogeneity, 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, pages 587–619, 2016

Decidability of the MC problem for HS

Theorem

The MC problem for full HS *over Kripke structures, under homogeneity, 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, pages 587–619, 2016

Theorem

The MC problem for full HS *with regular expressions over Kripke structures is decidable (with a non-elementary algorithm)*

Reference

L. Bozzelli, A. Molinari, A. Montanari, and A. Peron. Model checking interval temporal logics with regular expressions.
Information and Computation, 2018

What about the lower bound?

EXPSPACE-hardness of BE: a polynomial-time reduction from a domino-tiling problem for grids with rows of single exponential length

Theorem

The MC problem for BE over Kripke structures (under homogeneity/with regular expressions) is EXPSPACE-hard.

Reference

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Which fragments of the interval temporal logic HS are tractable in model checking?
Theoretical Computer Science, 2018

What about the lower bound?

EXPSPACE-hardness of BE: a polynomial-time reduction from a domino-tiling problem for grids with rows of single exponential length

Theorem

The MC problem for BE over Kripke structures (under homogeneity/with regular expressions) is EXPSPACE-hard.

Reference

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Which fragments of the interval temporal logic HS are tractable in model checking?
Theoretical Computer Science, 2018

The exact complexity of MC for BE is a difficult problem we are working on (BE is strictly in between Venema's CDT and the logic D of the sub-interval relation)

The MC problem for *HS* fragments: the logic $A\overline{A}B\overline{\overline{B}E}$

Let us consider the case of the logic $A\overline{A}B\overline{\overline{B}E}$, which is obtained from full HS ($A\overline{A}BE\overline{\overline{B}E}$) by removing modality $\langle E \rangle$

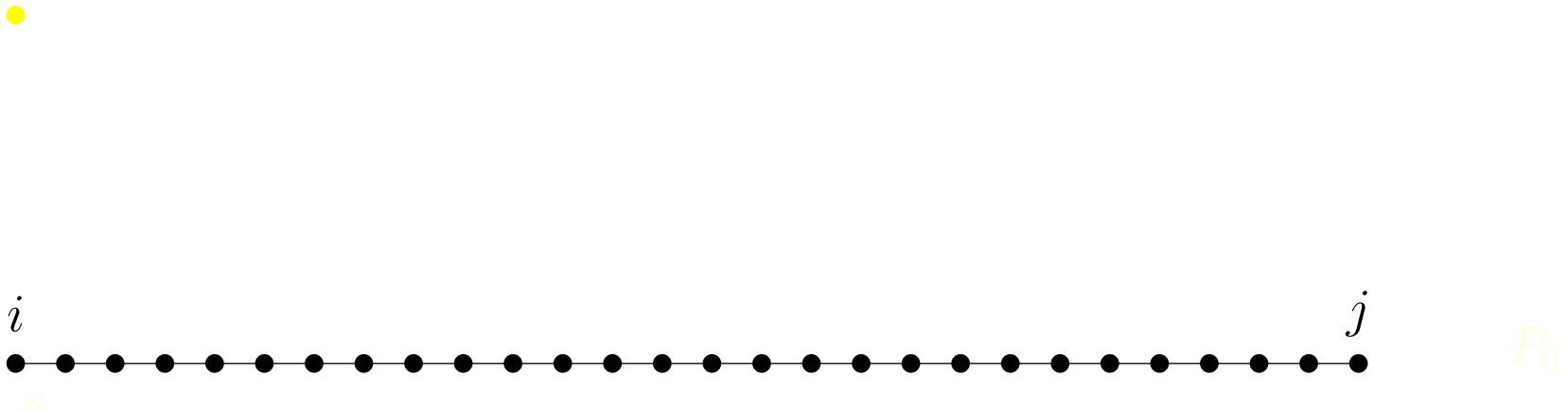
The MC problem for *HS* fragments: the logic $A\overline{A}B\overline{\overline{B}E}$

Let us consider the case of the logic $A\overline{A}B\overline{\overline{B}E}$, which is obtained from full HS ($A\overline{A}BE\overline{\overline{B}E}$) by removing modality $\langle E \rangle$

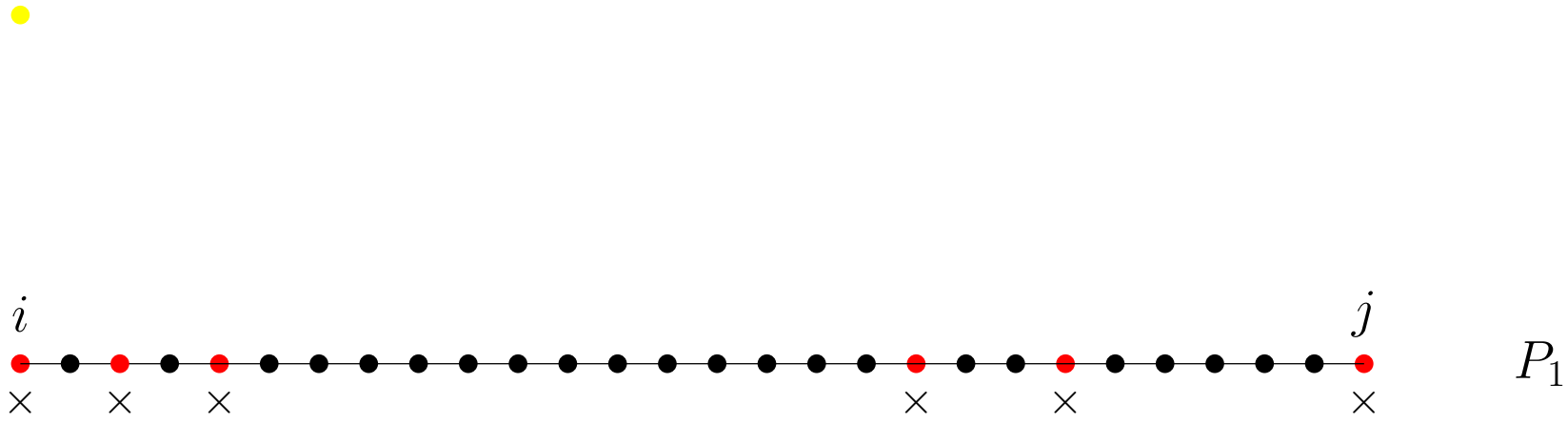
A high-level account of the solution:

- we can restrict our attention to 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 use in MC algorithms
- a trace representative can be chosen to represent a (possibly infinite) set of traces associated 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 h of the formula to check, can be given to the length of trace representatives

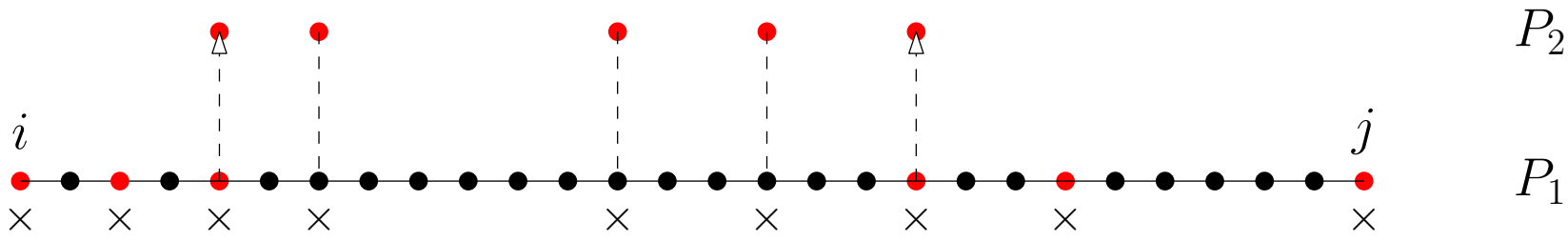
The basic idea: h-prefix sampling



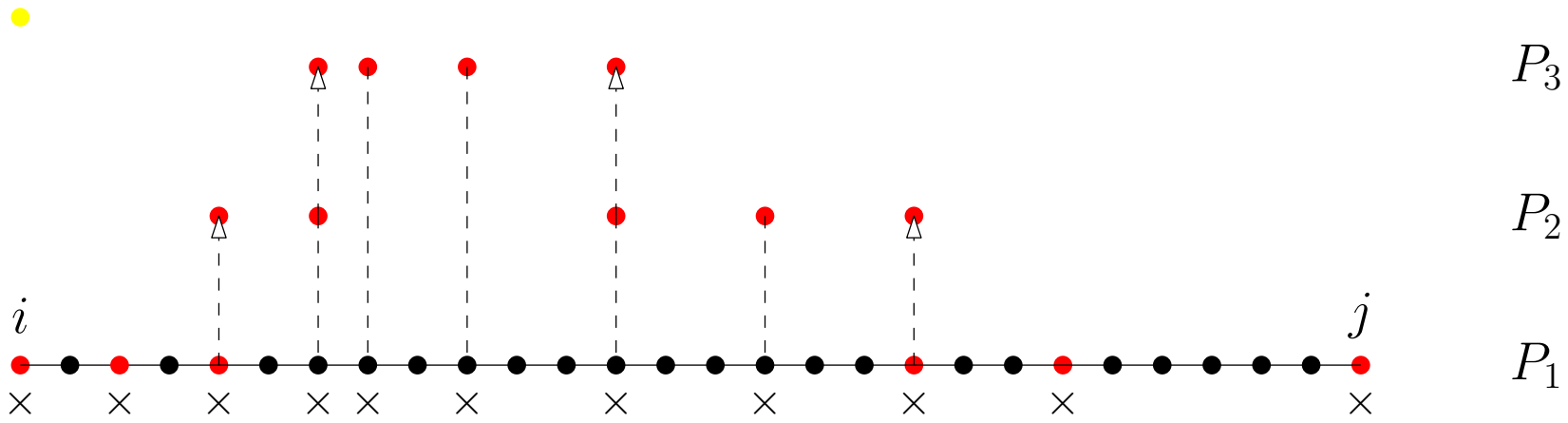
The basic idea: *h*-prefix sampling



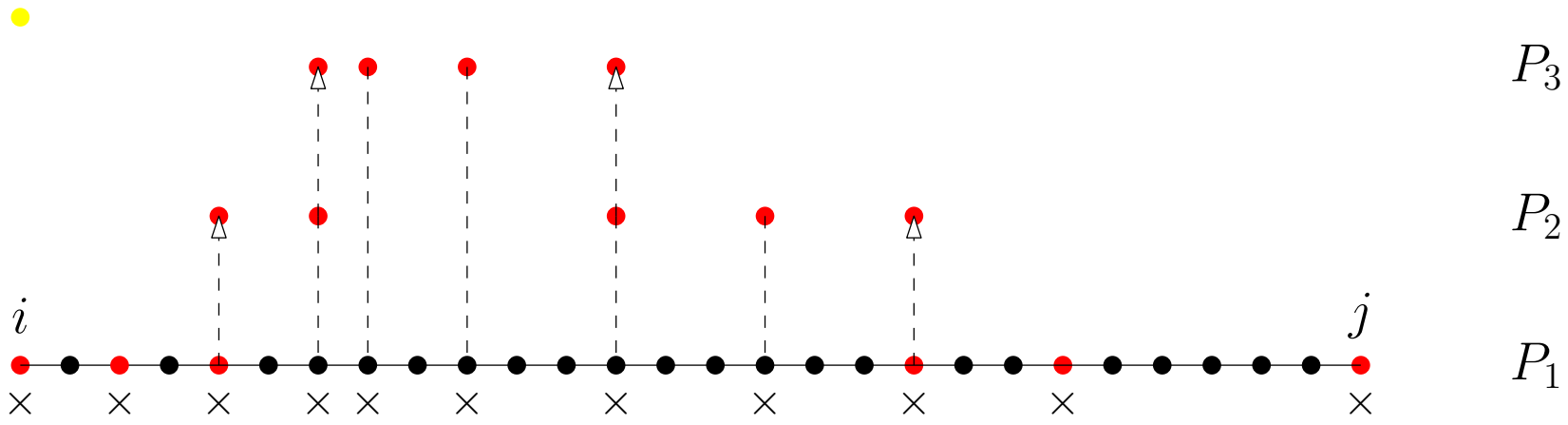
The basic idea: *h*-prefix sampling



The basic idea: *h*-prefix sampling



The basic idea: *h*-prefix sampling



Proposition

The h-prefix sampling P_h of (any) trace ρ is such that $|P_h| \leq (|W| + 2)^h$.

An EXPSPACE MC algorithm for $A\overline{A}B\overline{B}\overline{E}$

Theorem (Small model/trace property)

Given a trace ρ, we can derive its trace representative ρ', $\mathsf{Nest}_B(\psi)$-equivalent to it, such that $|\rho'| \leq (|W| + 2)^{\mathsf{Nest}_B(\psi)+2}$

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

1: $h \leftarrow \mathsf{Nest}_B(\psi)$
2: **for** all initial traces ρ' with $|\rho'| \leq (|W| + 2)^{h+2}$ **do**
3: **if** $\mathtt{Check}(\mathcal{K}, h, \psi, \rho') = 0$ **then return** 0: "$\mathcal{K}, \rho' \not\models \psi$" ◂ *Counterex* ✗
return 1: "$\mathcal{K} \models \psi$" ◂ *MC OK* ✓

Reference

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Which fragments of the interval temporal logic HS are tractable in model checking?
Theoretical Computer Science, 2018

Complexity results

	Homogeneity
Full *HS*, BE	non-elementary **EXPSPACE**-hard
$A\overline{A}B\overline{B}\overline{E}$, $A\overline{A}E\overline{B}\overline{E}$	$\in$ **AEXP**$_{\text{Pol}}$ **PSPACE**-hard
$A\overline{A}B\overline{E}$	**PSPACE**-complete
$A\overline{A}B\overline{B}$, $B\overline{B}$, $\overline{B}$, $A\overline{A}E\overline{E}$, $E\overline{E}$, $\overline{E}$	**PSPACE**-complete
$A\overline{A}B$, $A\overline{A}E$, AB, $\overline{A}E$	$\mathbf{P}^{\mathbf{NP}}$-complete
$A\overline{A}$, $\overline{A}B$, AE, A, $\overline{A}$	$\in \mathbf{P}^{\mathbf{NP}[O(\log^2 n)]}$ $\mathbf{P}^{\mathbf{NP}[O(\log n)]}$-hard
Prop, B, E	**co-NP**-complete

Complexity results

	Homogeneity	Regular expressions
Full *HS*, BE	non-elementary **EXPSPACE**-hard	non-elementary **EXPSPACE**-hard
$A\overline{A}B\overline{B}\overline{E}$, $A\overline{A}E\overline{B}\overline{E}$	$\in$ **AEXP**$_{\text{Pol}}$ **PSPACE**-hard	**AEXP**$_{\text{Pol}}$-complete
$A\overline{A}\overline{B}\overline{E}$	**PSPACE**-complete	$\in$ **AEXP**$_{\text{Pol}}$ **PSPACE**-hard
$A\overline{A}B\overline{B}$, $B\overline{B}$, $\overline{B}$, $A\overline{A}E\overline{E}$, $E\overline{E}$, $\overline{E}$	**PSPACE**-complete	**PSPACE**-complete
$A\overline{A}B$, $A\overline{A}E$, AB, $\overline{A}E$	$\mathbf{P}^{\mathbf{NP}}$-complete	**PSPACE**-complete
$A\overline{A}$, $\overline{A}B$, AE, A, $\overline{A}$	$\in \mathbf{P}^{\mathbf{NP}[O(\log^2 n)]}$ $\mathbf{P}^{\mathbf{NP}[O(\log n)]}$-hard	**PSPACE**-complete
Prop, B, E	**co-NP**-complete	**PSPACE**-complete

Complexity results

Reference

A. Molinari, A. Montanari, and A. Peron. Model checking for fragments of halpern and shoham's interval temporal logic based on track representatives.
Information and Computation, 259:412–443, 2018

Reference

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Which fragments of the interval temporal logic HS are tractable in model checking?
Theoretical Computer Science, 2018

Reference

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Model checking for fragments of the interval temporal logic HS at the low levels of the polynomial time hierarchy.
Information and Computation, 262:241–264, 2018

Point vs. interval temporal logic MC

Question: is there any advantage in replacing points by intervals as the primary temporal entities, or is it just a matter of taste?

Point vs. interval temporal logic MC

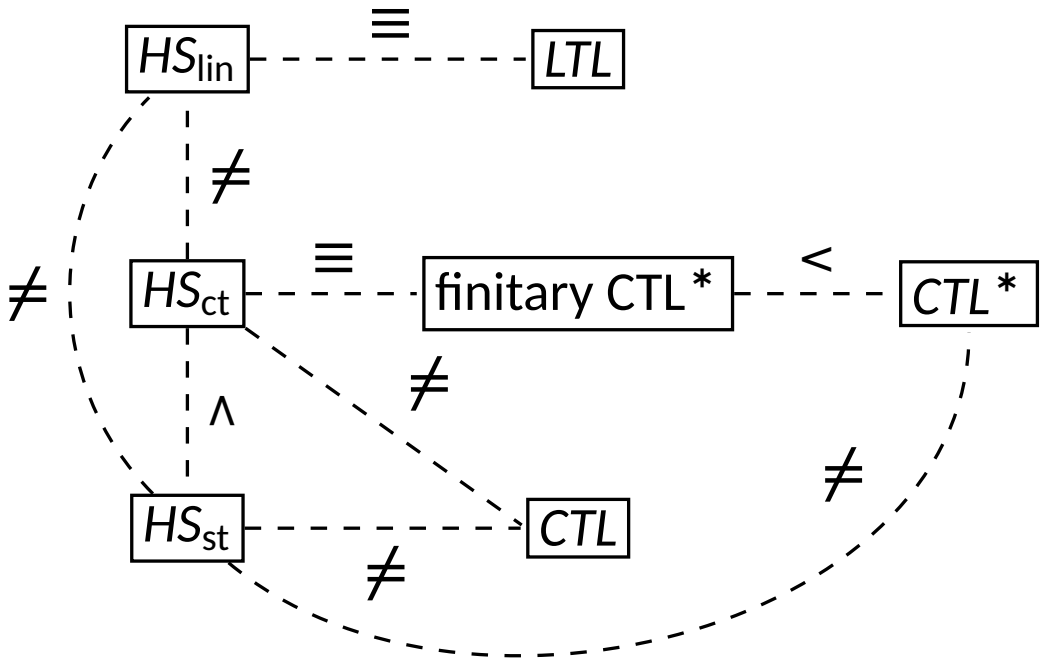
Question: is there any advantage in replacing points by intervals as the primary temporal entities, or is it just a matter of taste?

In order to compare the expressiveness of HS in MC with that of LTL, CTL, and CTL*, we consider three semantic variants of HS:

- HS with state-based semantics (the original one);
- HS with computation-tree-based semantics;
- HS with trace-based semantics.

These variants are compared with the above standard temporal logics and among themselves.

Expressiveness results (under homogeneity)



Reference

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Interval vs. point temporal logic model checking: an expressiveness comparison. *ACM Transactions on Computational Logic*, 2018

Towards more general system models

We are looking for possible replacements of Kripke structures by more expressive system models:

- interval-based system models, that allow one to directly describe systems on the basis of their interval behavior/properties (e.g., timelines).
- visibly pushdown systems, that can encode recursive programs and infinite state systems;

Reference

L. Bozzelli, A. Molinari, A. Montanari, and A. Peron. Decidability and Complexity of Timeline-based Planning over Dense Temporal Domains.
In *KR*, 2018

Reference

L. Bozzelli, A. Molinari, A. Montanari, and A. Peron. Complexity of timeline-based planning over dense temporal domains: exploring the middle ground.
In *GandALF*, 2018