LOG | COLLOQUIUM

July 23–28
Udine, Italy 2018

Model Checking: the Interval Way

Alberto Molinari (j.w. with L. Bozzelli, A. Montanari, A. Peron, P. Sala)
University of Udine
Department of Mathematics, Computer Science, and Physics (DMIF)

July 27, 2018

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 MC

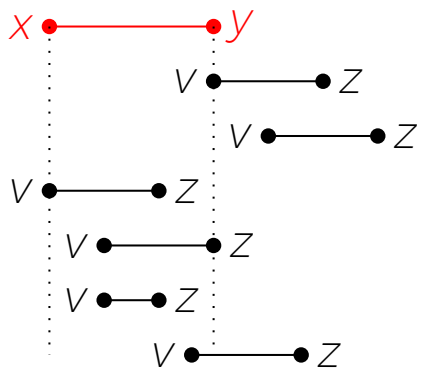
- Model checking (MC) is usually point-based:
  - properties express requirements over points (snapshots) of a computation (states of the state-transition system)
  - they are specified by means of point-based temporal logics such as LTL, CTL, and CTL*.

- 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 (e.g., HS)
    - ability to express: actions with duration, accomplishments, aggregations
    - applied to computational linguistics, artificial intelligence, temporal databases, formal verification

THE LOGIC HS

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

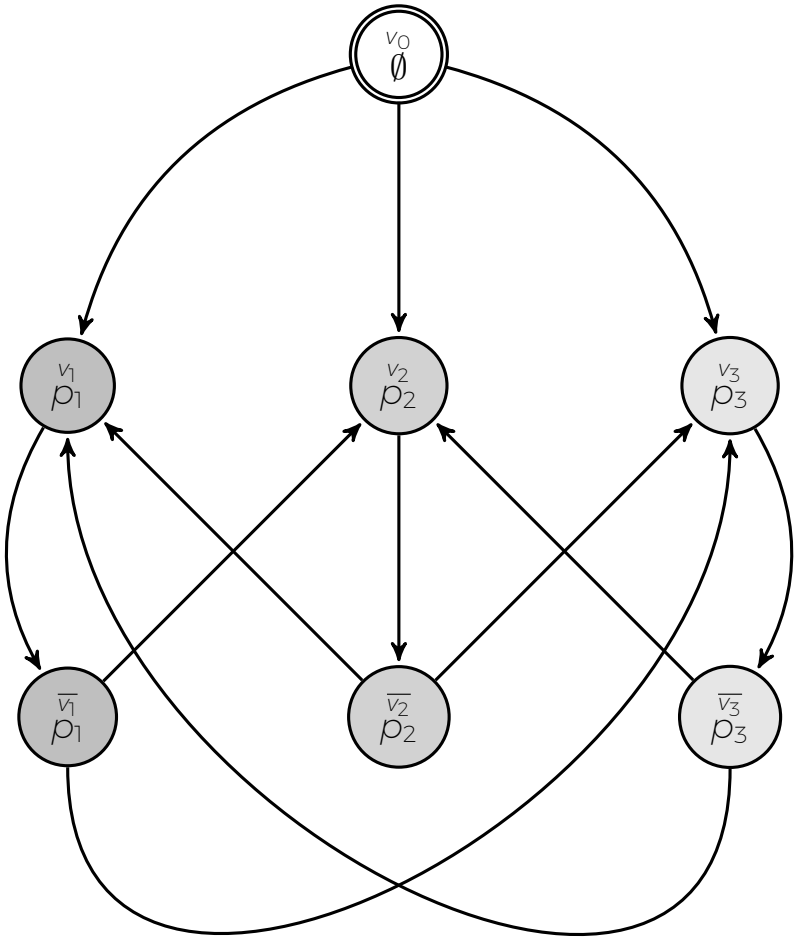
Allen rel.	HS	Definition	Example
meets	$\langle \mathsf{A} \rangle$	$[x,y]\mathcal{R}_A[v,z] \iff y = v$	
before	$\langle \mathsf{L} \rangle$	$[x,y]\mathcal{R}_L[v,z] \iff y < v$	
started-by	$\langle \mathsf{B} \rangle$	$[x,y]\mathcal{R}_B[v,z] \iff x = v \wedge z < y$	
finished-by	$\langle \mathsf{E}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



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

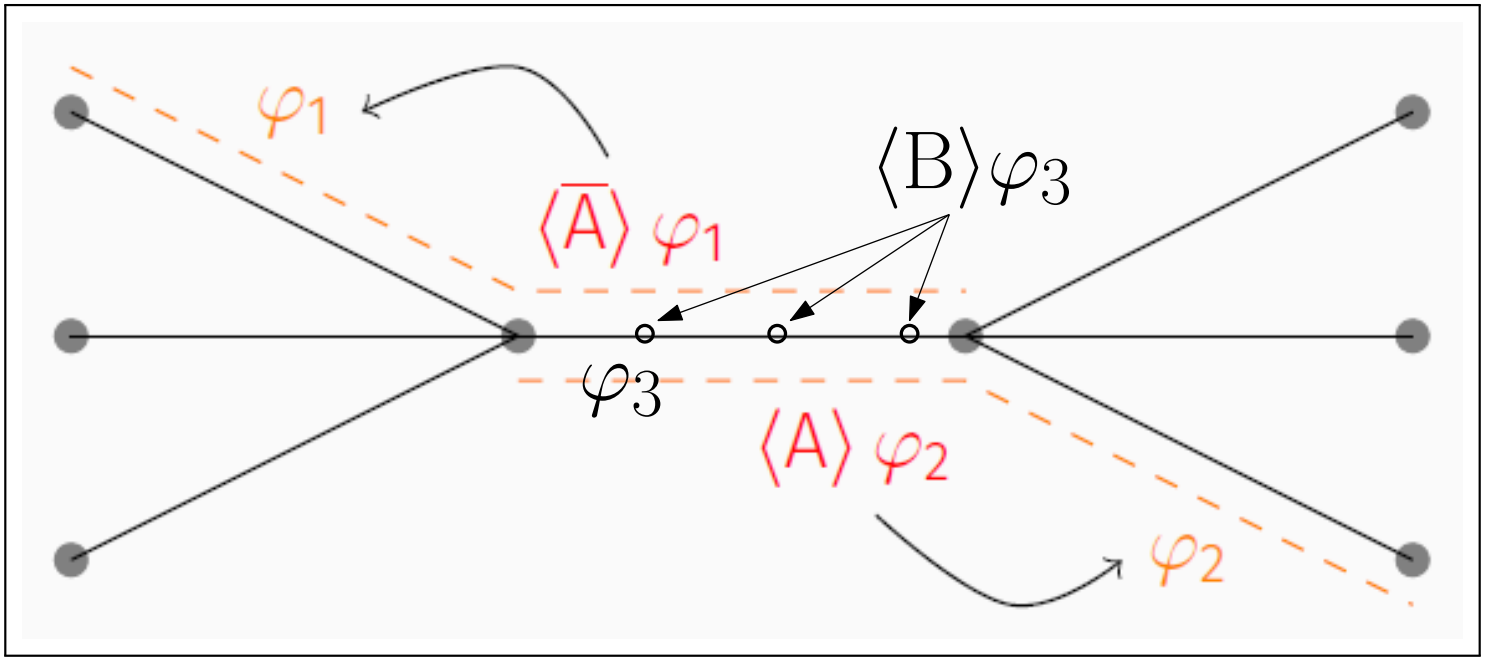
All modalities can be expressed by means of $\langle \mathsf{A} \rangle$, $\langle \mathsf{B} \rangle$, $\langle \mathsf{E} \rangle$ and their transposed modalities $\langle \overline{\mathsf{A}} \rangle$, $\langle \overline{\mathsf{B}} \rangle$, $\langle \overline{\mathsf{E}} \rangle$ only

KRIPKE STRUCTURES



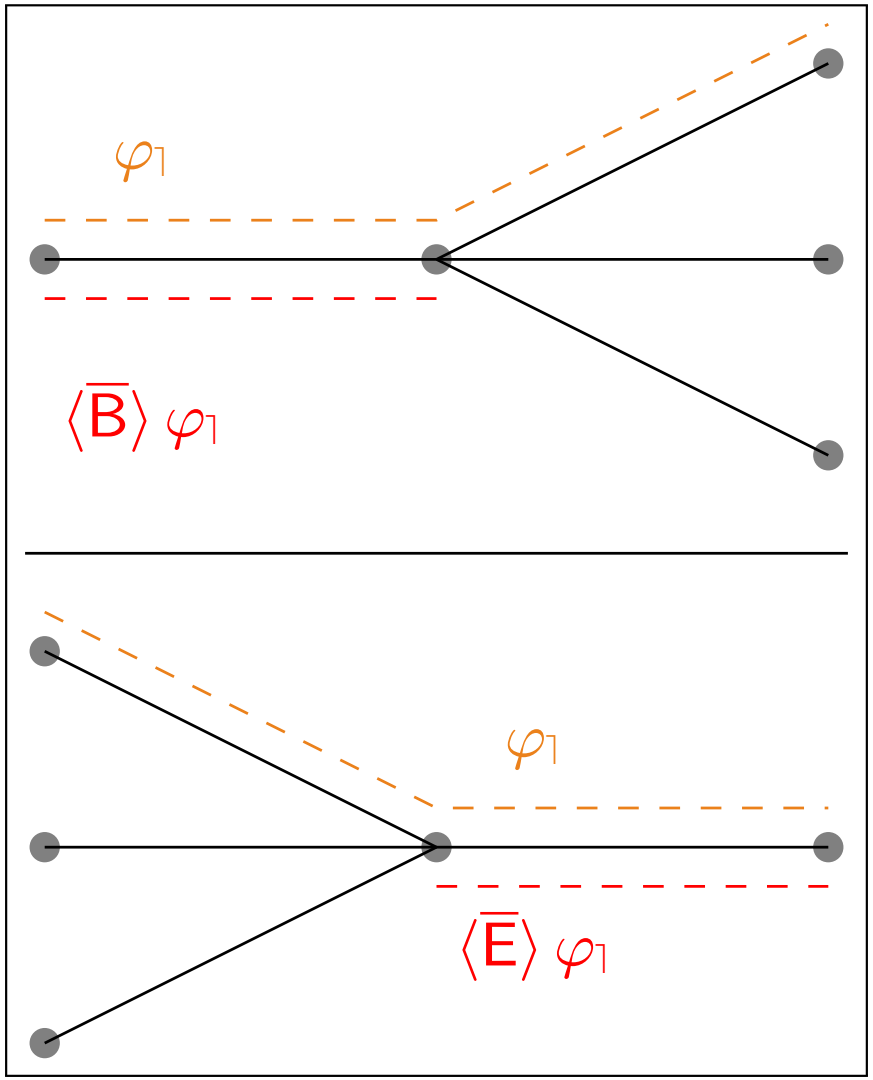
- HS formulas are interpreted over (finite) state-transition systems whose states are labeled with sets of proposition letters (Kripke structures)
- An interval is a trace (finite path) in a Kripke structure

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 $\mathcal{K} = (\mathcal{AP}, W, \delta, \mu, w_0)$:

- $\mathcal{K}, \rho \models p$ iff $p \in \bigcap_{w \in \mathsf{states}(\rho)} \mu(w)$, for any letter $p \in \mathcal{AP}$ (homogeneity assumption);

HS (STATE-BASED) SEMANTICS AND MC

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

- $\mathcal{K}, \rho \models p$ 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 $\mathcal{K} = (\mathcal{AP}, W, \delta, \mu, w_0)$:

- $\mathcal{K}, \rho \models r$ iff $\mu(\rho) \in \mathcal{L}(r)$
  (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 $\mathcal{K} = (\mathcal{AP}, W, \delta, \mu, w_0)$:

- $\mathcal{K}, \rho \models r$ iff $\mu(\rho) \in \mathcal{L}(r)$ (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 $\mathcal{K} = (\mathcal{AP}, W, \delta, \mu, w_0)$:

- $\mathcal{K}, \rho \models r$ iff $\mu(\rho) \in \mathcal{L}(r)$ (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

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

Possibly infinitely many traces!

HS (STATE-BASED) SEMANTICS AND MC

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

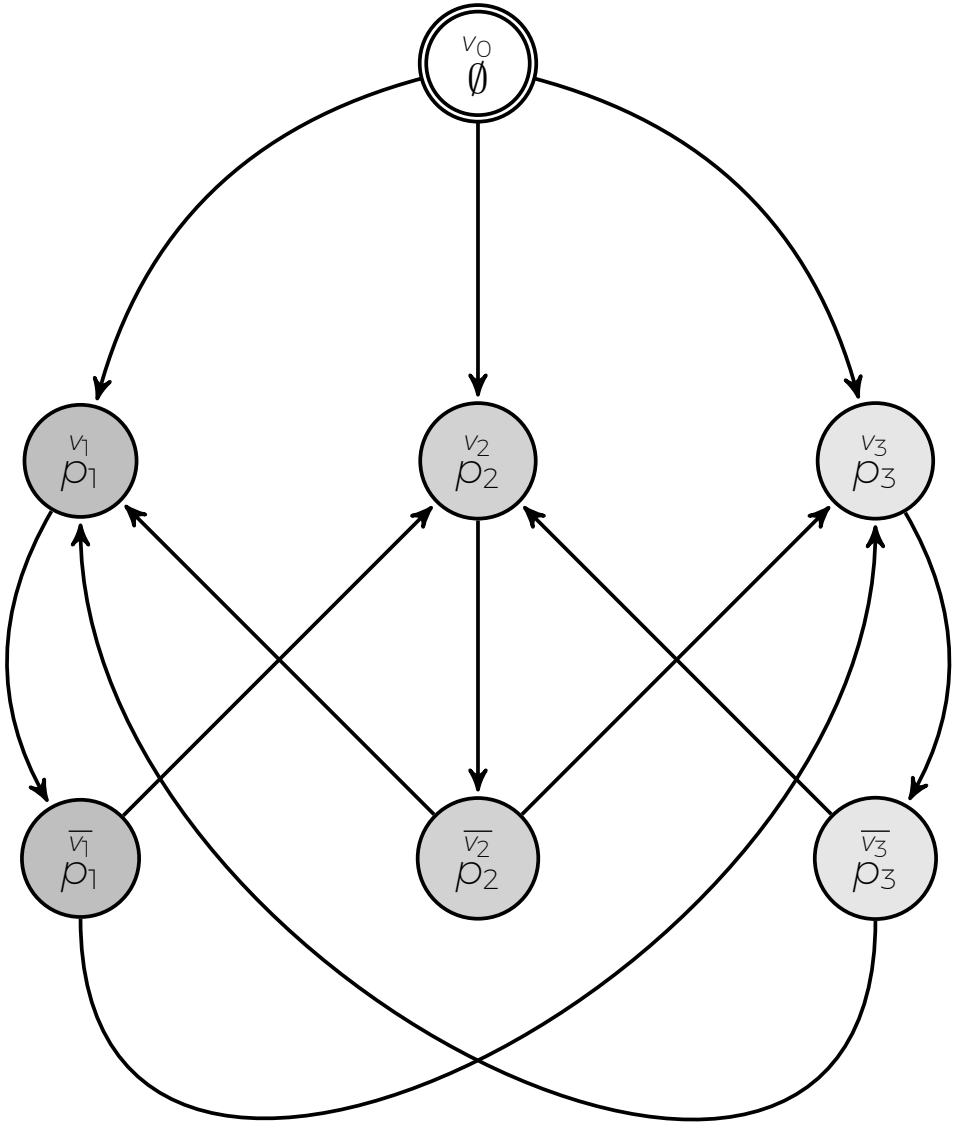
- $\mathcal{K}, \rho \models r$ iff $\mu(\rho) \in \mathcal{L}(r)$ (labeling based on regular expressions, subsuming the others);
- negation, disjunction, and conjunction are standard;
- $\mathcal{K}, \rho \models \langle \mathsf{A} \rangle \psi \ldots$;
- $\mathcal{K}, \rho \models \langle \mathsf{B}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

MC

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

Possibly infinitely many traces!

THE KRIPKE STRUCTURE $\mathcal{K}_{SCHED}$ FOR A SIMPLE SCHEDULER



A SHORT ACCOUNT OF $\mathcal{K}_{SCHED}$

$\mathcal{K}_{Sched}$ models the behaviour of a scheduler serving 3 processes which are continuously requesting the use of a common resource (easily generalizable to an arbitrary number of processes)

Initial state: v_0 (no process is served in that state)

In v_i and $\overline{v}_i$ the i-th process is served (p_i holds in those states)

The scheduler cannot serve the same process twice in two successive rounds:

- process i is served in state v_i, then, after "some time", a transition u_i from v_i to $\overline{v}_i$ is taken; subsequently, process i cannot be served again immediately, as v_i is not directly reachable from $\overline{v}_i$
- a transition r_j, with $j \neq i$, from $\overline{v}_i$ to v_j is then taken and process j is served

SOME PROPERTIES TO BE CHECKED OVER $\mathcal{K}_{SCHED}$

Validity of properties over all reachable computation intervals can be forced by modality $[E]$ (they are suffixes of at least one initial trace).

- In any computation interval of length at least 4, at least 2 processes are witnessed (YES: no process can be executed twice in a row)

$$\mathcal{K}_{Sched} \models [E](\langle \mathsf{E} \rangle^3 \top \rightarrow (\chi(p_1, p_2) \vee \chi(p_1, p_3) \vee \chi(p_2, p_3))),$$

  where $\chi(p, q) = \langle \mathsf{E} \rangle \langle \overline{\mathsf{A}} \rangle p \wedge \langle \mathsf{E} \rangle \langle \overline{\mathsf{A}} \rangle q$.

- In any computation interval of length at least 11, process 3 is executed at least once (NO: the scheduler can postpone the execution of a process ad libitum—starvation)

$$\mathcal{K}_{Sched} \not\models [E](\langle \mathsf{E} \rangle^{10} \top \rightarrow \langle \mathsf{E} \rangle \langle \overline{\mathsf{A}} \rangle p_3).$$

- In any computation interval of length at least 6, all processes are witnessed (NO: the scheduler should be forced to execute them in a strictly periodic manner, which is not the case)

$$\mathcal{K}_{Sched} \not\models [E](\langle \mathsf{E} \rangle^5 \rightarrow (\langle \mathsf{E} \rangle \langle \overline{\mathsf{A}} \rangle p_1 \wedge \langle \mathsf{E} \rangle \langle \overline{\mathsf{A}} \rangle p_2 \wedge \langle \mathsf{E} \rangle \langle \overline{\mathsf{A}} \rangle p_3)).$$

MC: THE KEY NOTION OF BE_K-DESCRIPTOR

- The BE-nesting depth of an HS formula ψ ($\mathsf{Nest}_{\mathsf{BE}}(\psi)$) 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 $\mathsf{Nest}_{\mathsf{BE}}(\psi) \leq k$

MC: THE KEY NOTION OF BE_K-DESCRIPTOR

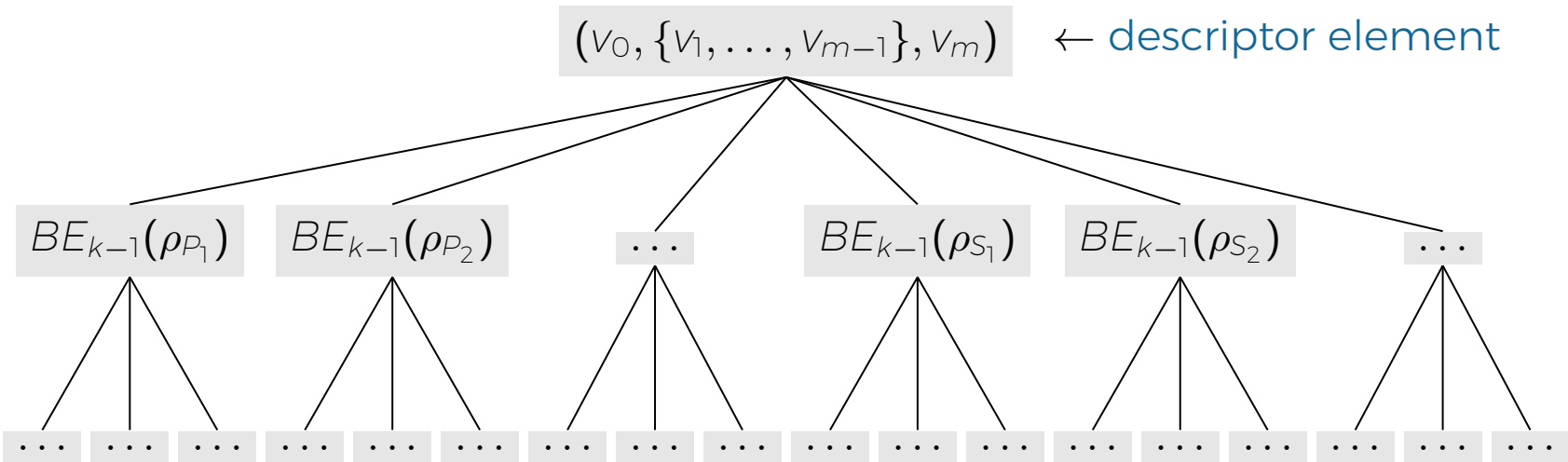
- The BE-nesting depth of an HS formula ψ ($\mathbf{Nest_{BE}}(\psi)$) is the maximum degree of nesting of modalities B and E in ψ
- Two traces ρ and ρ' of a Kripke structure $\mathcal{K}$ are k-equivalent iff:

$$\mathcal{K}, \rho \models \psi \text{ iff } \mathcal{K}, \rho' \models \psi \text{ for all HS formulas } \psi \text{ with } \mathbf{Nest_{BE}}(\psi) \leq k$$

For any given k, we provide a suitable tree representation for a trace, called a BE_k-descriptor

MC: THE KEY NOTION OF BE_K-DESCRIPTOR

The BE_k-descriptor for a trace $\rho = v_0 v_1 \ldots v_{m-1}\ v_m$, denoted $BE_k(\rho)$, has the following structure:

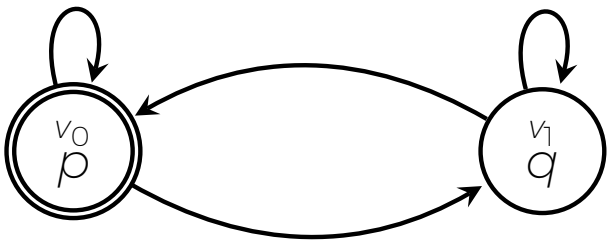


↑ $\rho_{P_1}, \rho_{P_2}, \ldots$ prefixes of ρ

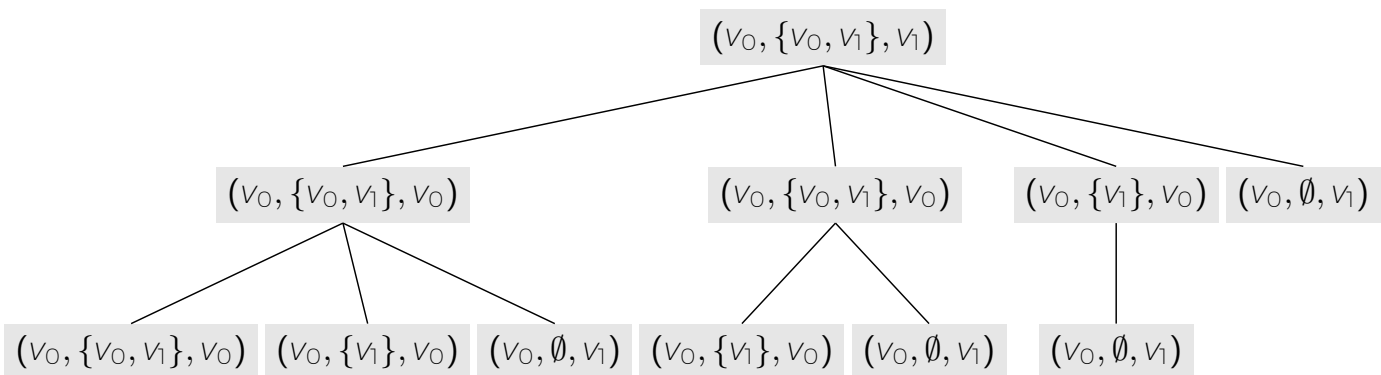
↑ $\rho_{S_1}, \rho_{S_2}, \ldots$ suffixes of ρ

Remark: the descriptor does not feature sibling isomorphic subtrees

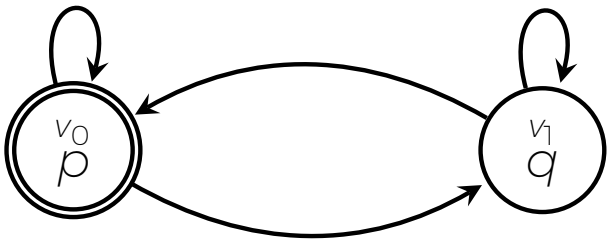
AN EXAMPLE OF A BE_2-DESCRIPTOR



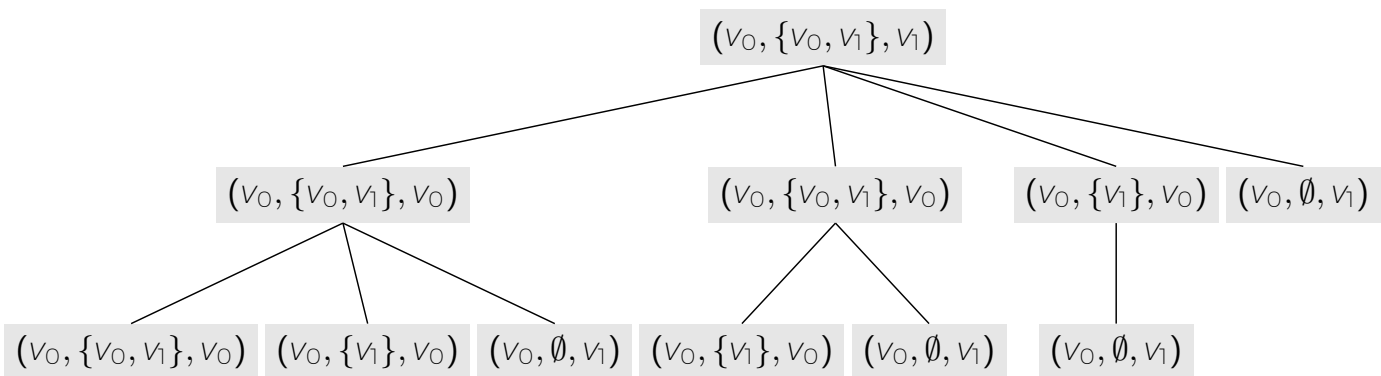
The BE_2-descriptor for the trace $\rho = v_0 v_1 v_0^4 v_1$ (for the sake of readability, only the subtrees for prefixes are displayed and point intervals are excluded)



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)

DECIDABILITY OF MC FOR FULL HS

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)

DECIDABILITY OF MC FOR FULL HS

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 HS MC

Theorem

The MC problem for full HS *over Kripke structures is decidable (nonelementary 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 HS MC

Theorem

The MC problem for full HS *over Kripke structures is decidable (nonelementary 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 BE *over Kripke structures is* **EXPSPACE***-hard*.

Reference

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*, pages 389–405, 2016

THE LOGIC $A\overline{A}B\overline{B}\overline{E}$

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

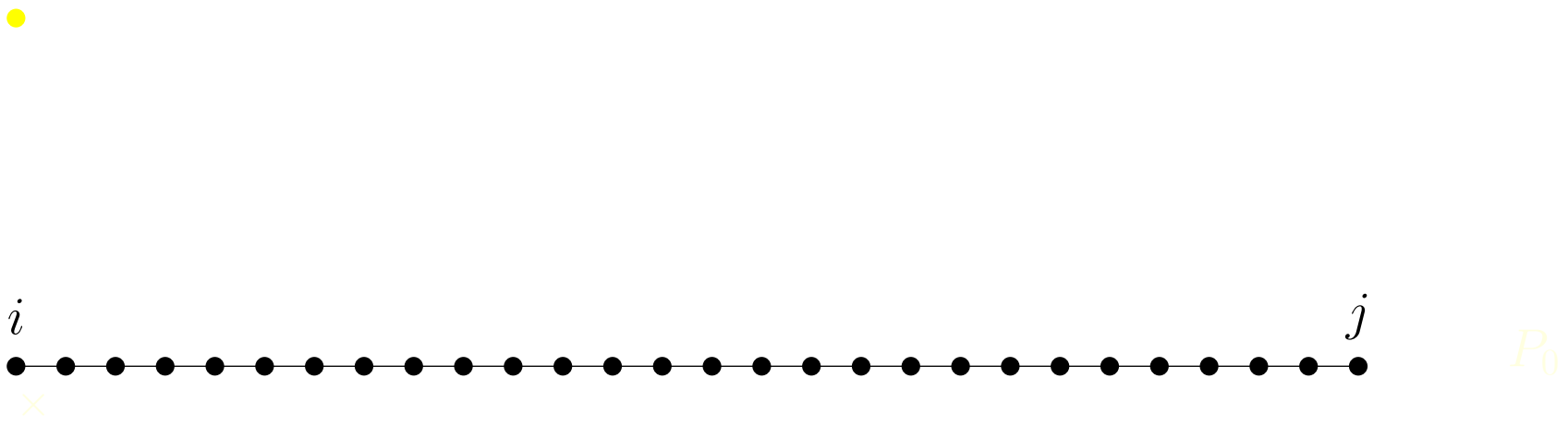
THE LOGIC $A\overline{A}B\overline{B}\overline{E}$

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

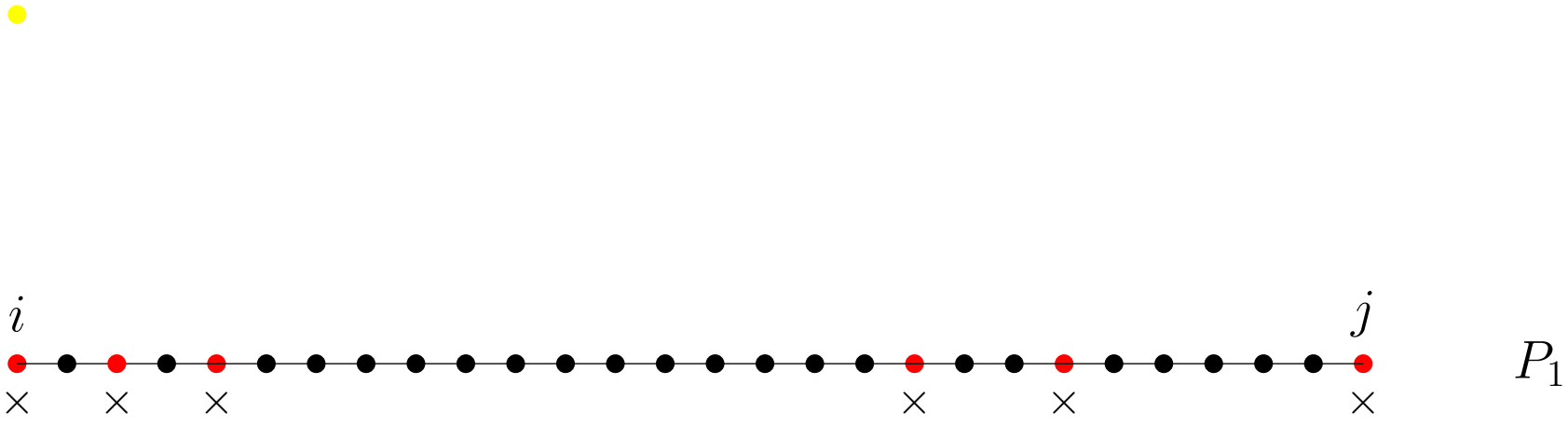
A high-level account of the solution:

- 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

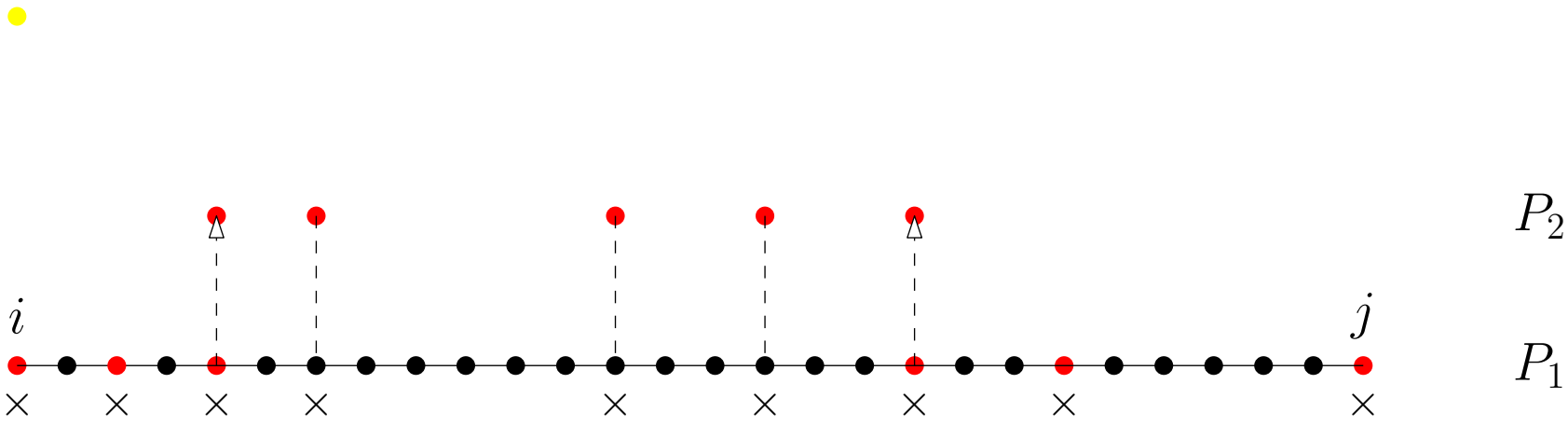
H-PREFIX SAMPLING



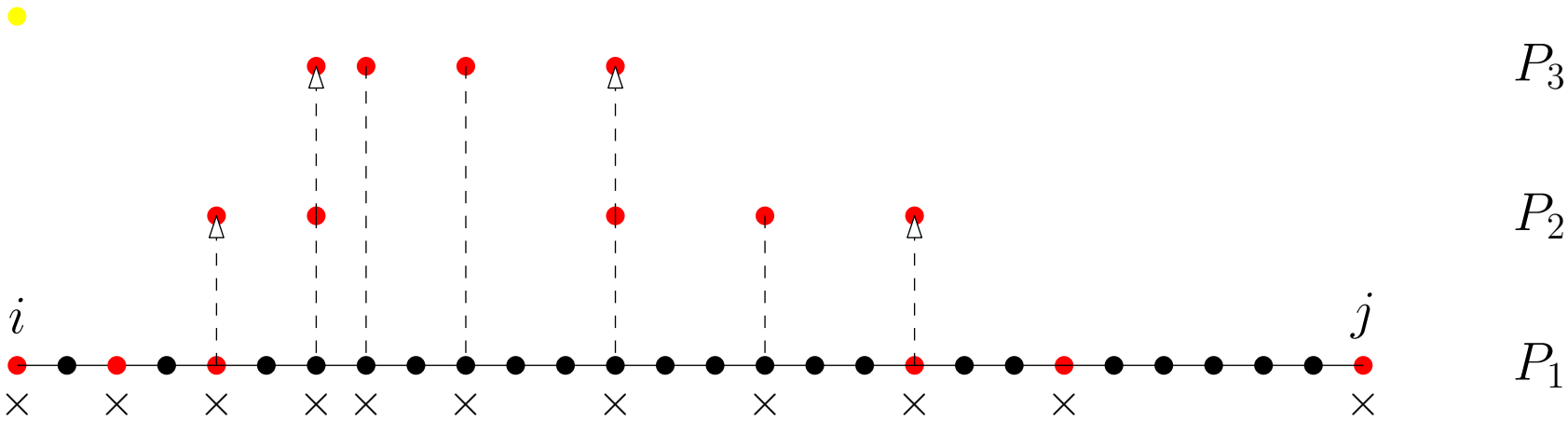
H-PREFIX SAMPLING



H-PREFIX SAMPLING



H-PREFIX SAMPLING



A SMALL-MODEL (TRACE) RESULT

- From a trace ρ, we can derive an h-equivalent trace ρ' 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 replace each $\rho(i,j)$ by another trace with no repeated occurrences of any state, except at most the first/last ones (hence no longer than $(|\mathcal{K}|+2)$).
- ρ and ρ' can be proved to be h-equivalent
- By the previous bound on $|P_{h+1}|$, we have $|\rho'| \leq (|\mathcal{K}|+2)^{h+2}$.

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 $|\rho'| \leq (|\mathcal{K}| + 2)^{\mathsf{Nest}_B(\psi)+2}$

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

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

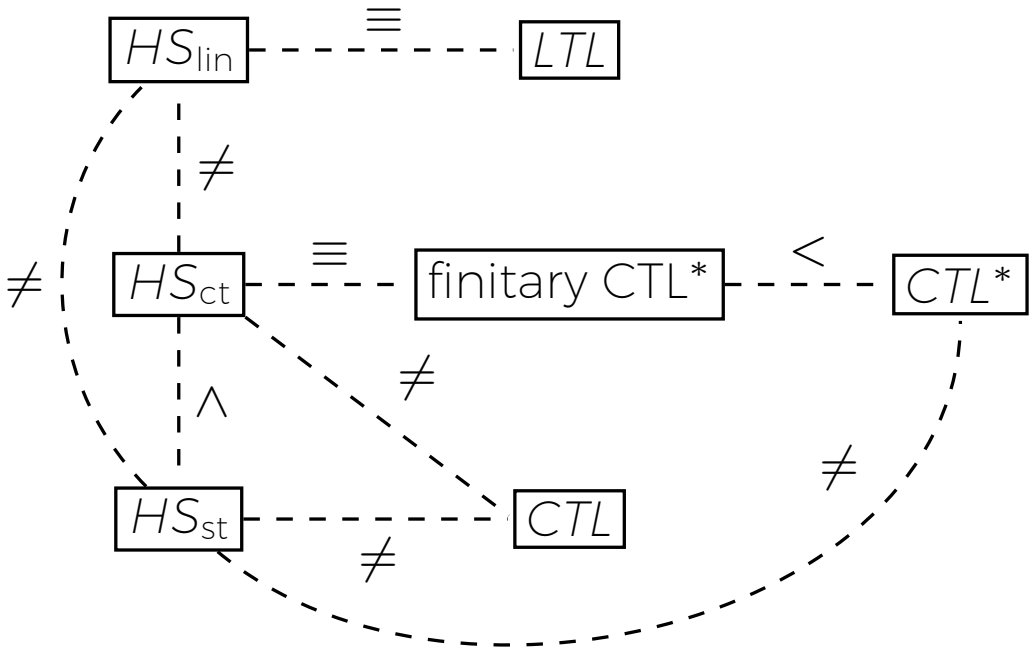
Reference

L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Interval temporal logic model checking based on track bisimilarity and prefix sampling.
In *ICTCS*, pages 49–61, 2016

COMPLEXITY RESULTS

	Homogeneity
Full *HS*, BE	non-elementary **EXPSPACE**-hard
$A\overline{A}B\overline{BE}$, $A\overline{A}E\overline{BE}$	$\in$ $\mathbf{AEXP}_{\mathbf{Pol}}$ **PSPACE**-hard
$A\overline{ABE}$	**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

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. In *FSTTCS*, 2016


L. Bozzelli, A. Molinari, A. Montanari, and A. Peron.
An in-depth investigation of interval temporal logic model checking with regular expressions.
In *SEFM*, pages 104–119, 2017.


L. Bozzelli, A. Molinari, A. Montanari, and A. Peron.
On the complexity of model checking for syntactically maximal fragments of the interval temporal logic HS with regular expressions.
In *GandALF*, pages 31–45, 2017.


L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala.
Interval temporal logic model checking based on track bisimilarity and prefix sampling.
In *ICTCS*, pages 49–61, 2016.


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*, pages 389–405, 2016.


L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala.
Interval vs. Point Temporal Logic Model Checking: an Expressiveness Comparison.
In *FSTTCS*, 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 $\mathbf{P}^{\mathbf{NP}}$-Complete.
In *GandALF*, pages 76–90, 2016.


L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala.
Satisfiability and model checking for the logic of sub-intervals under the homogeneity assumption.
In *ICALP*, pages 120:1–120:14, 2017.


A. Molinari, A. Montanari, A. Murano, G. Perelli, and A. Peron.
Checking interval properties of computations.
Acta Informatica, pages 587–619, 2016.


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, and A. Peron.
Constraining cycle alternations in model checking for interval temporal logic.
In *ICTCS*, pages 211–226, 2016.


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.


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.