Complexity Analysis of a Unifying Algorithm for Model Checking Interval Temporal Logic

Laura Bozzelli
University of Napoli "Federico II", Napoli, Italy

Angelo Montanari
University of Udine, Udine, Italy

Adriano Peron
University of Napoli "Federico II", Napoli, Italy

Abstract

The model-checking (MC) problem of Halpern and Shoham Interval Temporal Logic (HS) has been recently investigated in some papers and is known to be decidable. An intriguing open question concerns the exact complexity of the problem for full HS: it is at least **EXPSPACE**-hard, while the only known upper bound is non-elementary and is obtained by exploiting an abstract representation of Kripke structure paths called *descriptors*. In this paper we generalize the approach by providing a uniform framework for model-checking full HS and meaningful (almost maximal) fragments, where a specialized type of descriptor is defined for each fragment. We then devise a general MC alternating algorithm parameterized by the type of descriptor which has a polynomially bounded number of alternations and whose running time is bounded by the length of minimal representatives of descriptors (certificates). We analyze the time complexity of the algorithm and give, by non-trivial arguments, tight bounds on the length of certificates. For two types of descriptors, we obtain exponential upper and lower bounds which lead to an elementary MC algorithm for the related HS fragments. For the other types of descriptors, we provide non-elementary lower bounds. This last result addresses a question left open in some papers regarding the possibility of fixing an elementary upper bound on the size of the descriptors for full HS.

2012 ACM Subject Classification Theory of computation → Logic and verification

Keywords and phrases Interval temporal logic, Model checking, Complexity and succinctness issues

Digital Object Identifier 10.4230/LIPIcs.TIME.2019.18

1 Introduction

Model checking (MC) is a well-established formal-method technique to automatically check for global correctness of finite-state reactive systems. Finite systems are usually modelled as labelled state-transition graphs (finite Kripke structures), while the properties of interest are specified in standard *Point-based* temporal logics (PTLs), such as, for instance, the linear-time temporal logic LTL [22] and the branching-time temporal logics CTL and CTL* [9]. *Interval temporal logics* (ITLs) provide an alternative setting for reasoning about time [11, 21, 25]. ITLs assume intervals, instead of points, as their primitive temporal entities allowing to specify relevant temporal properties that involve, e.g., actions with duration, accomplishments, and temporal aggregations, which are inherently "interval-based", and thus cannot be naturally expressed by PTLs. ITLs find applications in a variety of computer science fields, including artificial intelligence (reasoning about action and change, qualitative reasoning, planning, and natural language processing), theoretical computer science (specification and verification of programs), and temporal and spatio-temporal databases (e.g. see [13, 21, 23]). Among ITLs, the landmark is *Halpern and Shoham's modal logic of time intervals* (HS) [11] which features one modality for each of the 13 possible ordering relations between pairs of intervals (the so-called Allen's relations [1]), apart from equality. The satisfiability problem for HS is undecidable over all relevant classes of linear orders, and most of its fragments (with some meaningful exceptions [7, 8, 20]) are undecidable as well [6, 12, 15].

Model checking of (finite) Kripke structures against HS has been investigated only very recently [13, 14, 16, 2, 5, 4, 3, 18, 19]. The idea is to interpret each finite path of a Kripke structure as an interval, whose labelling is defined on the basis of the labelling of the component states: a proposition letter holds over an interval if and only if it holds over each component state (*homogeneity assumption* [24]). In this paper, we focus on the MC problem of HS under the *state-based semantics* (time branches both in the future and in the past) proved decidable in [16]. In this setting, the temporal modalities for the Allen's relations *started-by* (B), *finished-by* (E), and *contains* (D), have a "linear-time" character: they allows to select either proper prefixes (B), or proper suffixes (E), or internal subpaths (D) of the current path. The modalities associated with the other Allen's relations are instead "branching-time": they allow *either* to non-deterministically extend a prefix (resp., suffix, resp., subpath) of the current path in the future or in the past, *or* to non-deterministically select an independent path whose start point (resp., ending point) is reachable from (resp., can reach) the ending point (resp., start point) of the current path. The expressiveness of the state-based semantics of HS has been studied in [5] together with two other decidable variants: the *computation-tree-based semantics*, that allows time to branch only in the future, and the *trace-based semantics*, that disallows time branching. The computation-tree-based variant of HS is expressively equivalent to finitary CTL* (the variant of CTL* with quantification over finite paths), while the trace-based variant is equivalent to LTL (but at least exponentially more succinct). The state-based variant is more expressive than the computation-tree-based variant and expressively incomparable with both LTL and CTL*.

As far as concerns the complexity of the state-based MC problem, for the full logic HS, the problem is at least **EXPSPACE**-hard [2], while the only known upper bound is non-elementary [16]. The approach for full HS [16] consists in defining a finite abstraction over the (possibly infinite) set of finite paths of a Kripke structure. This abstraction is parameterized by a natural number h and is based on the *h-level BE-descriptor* of a path: a tree-like structure of depth h which conveys information about the states occurring in prefixes and suffixes of the path. Paths having the same h-level BE-descriptor (i) are indistinguishable with respect to the fulfillment of HS formulas having nesting depth of modalities for prefixes (B) and suffixes (E) at most h, and (ii) admit a bounded minimal representative (*h-level BE-certificate*) whose length is at most a tower of exponentials of height h. The model-checking procedure for full HS based on BE-descriptors is only sketched in [16] and, in particular, the succinctness of BE-descriptors has not been investigated so far. In subsequent papers [3, 19, 4, 17], the focus has been on some syntactical fragments of HS: the fragment featuring only the modalities for the *contains* relation (D), and fragments featuring modalities for a subset of the Allen relations *meets* (A), *started-by* (B), *finished-by* (E) and their transposed relations $\overline{A}$, $\overline{B}$, and $\overline{E}$, respectively (see Table 1 for a graphical intuition of relations). The complete picture of known results is reported in Figure 1.

In this paper, we first provide a uniform framework for the state-based MC problem against the HS syntactical fragments obtained by combining the modalities of a linear-time basis $\mathcal{B}$ (i.e, a non-empty subset of non-interdefinable Allen's relations in $\{B, E, D\}$) with the modalities for the (branching-time) Allen's relations in $\{A, L, O, \overline{A}, \overline{L}, \overline{B}, \overline{E}, \overline{D}, \overline{O}\}$ but not including either the modalities for *overlap* O or the modalities of its transposed relation $\overline{O}$ (the fragment for the complete basis $\{B, E\}$ expresses the full logic HS). The proposed approach generalizes the one provided in [16], where only the full logic HS is considered: for each basis $\mathcal{B}$, it defines a finite abstraction of the set of paths of a Kripke structure based on the notion of *h-level $\mathcal{B}$-descriptor* (coinciding with the BE-descriptor for the complete basis $\mathcal{B} = \{B, E\}$). As for the basis $\{B, E\}$, we show that for all the other bases with

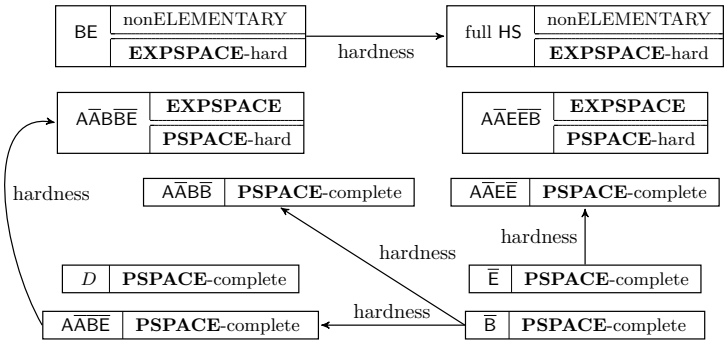


Figure 1 Complexity of the MC problem for HS fragments.

the exception of $\{D\}$, paths having the same h-level $\mathcal{B}$-descriptor (i) are indistinguishable with respect to the fulfillment of HS formulas having nesting depth of modalities for $\mathcal{B}$ at most h, and (ii) admit a bounded minimal representative (*h-level $\mathcal{B}$-certificate*). We exploit these results for devising an *alternating* algorithm, parameterized in the basis $\mathcal{B} \neq \{D\}$, for model-checking the associated fragment, which runs in time bounded by the maximal length of h-level $\mathcal{B}$-certificates of the input Kripke structure, with h being the $\mathcal{B}$-nesting depth of the input formula, and whose number of alternations between existential and universal choices is at most the size of the input formula.

As a second contribution, for each basis $\mathcal{B}$, we provide tight bounds on the length of h-level $\mathcal{B}$-certificates. For the bases $\{B\}$ and $\{E\}$, we prove singly-exponential upper and lower bounds. Hence, by the proposed alternating algorithm, we argue that model-checking for the fragments $\mathsf{A\overline{A}B\overline{B}D\overline{E}L\overline{L}O}$ and $\mathsf{A\overline{A}B\overline{D}E\overline{E}L\overline{L}O}$ is in the complexity class $\mathbf{AEXP_{pol}}$ of problems decided by exponential-time bounded alternating Turing Machines with a polynomially bounded number of alternations (a class included in **EXPSPACE** which captures the precise complexity of some relevant problems, e.g., the first-order theory of real addition with order [10]). On the other hand, for all bases $\mathcal{B}$ distinct from $\{B\}$ and $\{E\}$, we state a non-elementary lower bound. In particular, the result obtained for the basis $\{B, E\}$ negatively answers a question left open in [16] regarding the possibility of fixing an elementary upper bound on the size of BE-descriptors, and at the same time provides new insight on the MC problem for full HS: if elementary procedures are possible, they have certainly to exploit less powerful structures than descriptors.

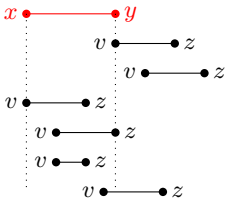
The paper is organised as follows. In Section 2, we recall the state-based model-checking framework for HS. In Section 3, we introduce for each basis $\mathcal{B}$, the notion of $\mathcal{B}$-descriptor, and describe the algorithm to solve the MC problem for the associated fragment. In Section 4, we fix tight bounds on the length of $\mathcal{B}$-certificates giving conclusions in Section 5.

2 Preliminaries

In this section, after introducing some notations we recall in Subsection 2.1 the logic HS [11] and the state-based model-checking framework for verifying HS formulas [16].

Let $\mathbb{N}$ be the set of natural numbers. For all $i, j \in \mathbb{N}$, with $i \leq j$, $[i, j]$ denotes the set of natural numbers h such that $i \leq h \leq j$. For all $n, h \in \mathbb{N}$, $\mathit{Tower}(n, h)$ denotes a tower of exponentials of height h and argument n: $\mathit{Tower}(n, 0) = n$ and $\mathit{Tower}(n, h+1) = 2^{\mathit{Tower}(n,h)}$. Let Σ be a finite alphabet. The set of all the finite words over Σ is denoted by Σ^*, and $\Sigma^+ := \Sigma^* \setminus \{\varepsilon\}$, where ε is the empty word. Let w be a finite word over Σ. We denote by $|w|$ the length of w. For all $i, j \in \mathbb{N}$, with $i \leq j$, $w(i)$ is the i-th letter of w ($w(0)$ is the first

Table 1 Allen's relations and corresponding HS modalities.

Allen relation	HS	Definition w.r.t. interval structures	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	$\langle O \rangle$	$[x,y]\mathcal{R}_O[v,z] \iff x < v < y < z$	

letter) while $w[i,j]$ denotes the infix of w given by $w(i)\cdots w(j)$. If $w \neq \varepsilon$, then we denote by $\mathsf{fst}(w)$ and $\mathsf{lst}(w)$ the first and last symbol of w, and by $\mathsf{internal}(w)$ the set of letters in Σ occurring in $w[1, n-1]$ where $|w| = n+1$. The concatenation of two finite words w and w' is denoted by $w \cdot w'$. Moreover, if $\mathsf{lst}(w) = \mathsf{fst}(w')$, $w \star w'$ represents $w[0, n-1] \cdot w'$, where $|w| = n+1$ ($\star$-concatenation). The set $\mathsf{Pref}(w)$ of *non-empty proper prefixes* of w is the set of non-empty finite words u such that $w = u \cdot v$ for some non-empty word v. The set $\mathsf{Suff}(w)$ of *non-empty proper suffixes* of w is the set of non-empty words u such that $w = v \cdot u$ for some non-empty finite word v. A *subword* (resp., *internal subword*) of w is a word w' such that w is of the form $w = u \cdot w' \cdot v$ for some words (resp., for some non-empty words) u and v.

2.1 The Interval Temporal Logic HS

An interval algebra to reason about intervals and their relative orders was proposed by Allen in [1], while a systematic logical study of interval representation and reasoning was done a few years later by Halpern and Shoham, who introduced the interval temporal logic HS featuring one modality for each Allen relation, but equality [11]. Table 1 depicts 6 of the 13 Allen's relations, together with the corresponding HS (existential) modalities. The other 7 relations are the 6 inverse relations (given a binary relation $\mathcal{R}$, the inverse relation $\overline{\mathcal{R}}$ is such that $b\overline{\mathcal{R}}a$ iff $a\mathcal{R}b$) and equality.

Let $\mathcal{AP}$ be a finite set of atomic propositions. HS formulas ψ over $\mathcal{AP}$ are defined as follows:

$$\psi ::= \top \mid \bot \mid p \mid \neg\psi \mid \psi \wedge \psi \mid \langle \mathrm{X} \rangle \psi$$

where $p \in \mathcal{AP}$ and $\langle \mathrm{X} \rangle$ is the existential temporal modality for the (non-trivial) Allen's relations $X \in \{A, L, B, E, D, O, \overline{A}, \overline{L}, \overline{B}, \overline{E}, \overline{D}, \overline{O}\}$. The size $|\psi|$ of a formula ψ is the number of distinct subformulas of ψ. We also exploit the standard logical connectives $\vee$ (disjunction) and $\rightarrow$ (implication) as abbreviations, and for any temporal modality $\langle \mathrm{X} \rangle$, the dual universal modality $[\mathrm{X}]$ defined as: $[\mathrm{X}]\,\psi := \neg\langle \mathrm{X} \rangle \neg\psi$. An HS formula ψ is in *positive normal form* (*PNF*) if negation is applied only to atomic formulas in $\mathcal{AP}$. By using De Morgan's laws and for any existential modality $\langle \mathrm{X} \rangle$, the dual universal modality $[\mathrm{X}]$, we can convert in linear-time an HS formula ψ into an equivalent formula in *PNF*, called the *PNF* of ψ. For a formula ψ in *PNF*, the *dual* $\widetilde{\psi}$ of ψ is the *PNF* of $\neg\psi$.

Given a set $U \subseteq \{A, L, B, E, D, O, \overline{A}, \overline{L}, \overline{B}, \overline{E}, \overline{D}, \overline{O}\}$ of Allen's relations, the *joint nesting depth of U in a formula* ψ denoted by $\mathrm{depth}_U(\psi)$ is defined as: (i) $\mathrm{depth}_U(p) = 0$, for any $p \in \mathcal{AP}$; (ii) $\mathrm{depth}_U(\neg\psi) = \mathrm{depth}_U(\psi)$; (iii) $\mathrm{depth}_U(\psi \wedge \varphi) = \max\{\mathrm{depth}_U(\psi), \mathrm{depth}_U(\varphi)\}$; (iv) $\mathrm{depth}_U(\langle \mathrm{X} \rangle \psi) = 1 + \mathrm{depth}_U(\psi)$ if $X \in U$, and $\mathrm{depth}_U(\langle \mathrm{X} \rangle \psi) = \mathrm{depth}_U(\psi)$ otherwise; (iv) $\mathrm{depth}_U([\mathrm{X}]\,\psi) = 1 + \mathrm{depth}_U(\psi)$ if $X \in U$, and $\mathrm{depth}_U([\mathrm{X}]\,\psi) = \mathrm{depth}_U(\psi)$ otherwise.

Given any subset of Allen's relations $\{X_1, .., X_n\}$, we denote by $\mathsf{X_1} \cdots \mathsf{X_n}$ the HS fragment featuring existential (and universal) modalities for $X_1, .., X_n$ only.

We assume the *non-strict semantics of HS*, which admits intervals consisting of a single point (all the results proved in the paper hold for the strict semantics as well). Under such an assumption, all HS-temporal modalities can be expressed in terms of $\langle \mathrm{B} \rangle, \langle \mathrm{E} \rangle, \langle \overline{\mathrm{B}} \rangle$, and $\langle \overline{\mathrm{E}} \rangle$ [25]. HS can thus be regarded as a multi-modal logic with $\langle \mathrm{B} \rangle, \langle \mathrm{E} \rangle, \langle \overline{\mathrm{B}} \rangle$, and $\langle \overline{\mathrm{E}} \rangle$ as primitive modalities and its semantics can be defined over a multi-modal Kripke structure, called *abstract interval model* (AIM for short), where intervals are treated as atomic objects and Allen's relations as binary relations over intervals.

▶ **Definition 1** (Abstract interval models [16]). *An* abstract interval model *(AIM) over $\mathcal{AP}$ is a tuple $\mathcal{A} = (\mathcal{AP}, \mathbb{I}, B_{\mathbb{I}}, E_{\mathbb{I}}, Lab_{\mathbb{I}})$, where $\mathbb{I}$ is a possibly infinite set of worlds (abstract intervals), $B_{\mathbb{I}}$ and $E_{\mathbb{I}}$ are two binary relations over $\mathbb{I}$, and $Lab_{\mathbb{I}} : \mathbb{I} \mapsto 2^{\mathcal{AP}}$ is a labeling function, which assigns a set of proposition letters from $\mathcal{AP}$ to each abstract interval.*

In the interval setting, $\mathbb{I}$ is interpreted as a set of intervals and $B_{\mathbb{I}}$ and $E_{\mathbb{I}}$ as Allen's relations B (*started-by*) and E (*finished-by*), respectively; $Lab_{\mathbb{I}}$ assigns to each interval in $\mathbb{I}$ the set of atomic propositions that hold over it. Given an interval $I \in \mathbb{I}$, the truth of an HS formula over I is inductively defined as follows (the Boolean connectives are treated as usual):

- $\mathcal{A}, I \models p$ if $p \in Lab_{\mathbb{I}}(I)$, for any $p \in \mathcal{AP}$;
- $\mathcal{A}, I \models \langle \mathrm{X} \rangle \psi$, for $X \in \{B, E\}$, if $I \, X_{\mathbb{I}} \, J$ and $\mathcal{A}, J \models \psi$ for some $J \in \mathbb{I}$;
- $\mathcal{A}, I \models \langle \overline{\mathrm{X}} \rangle \psi$, for $\overline{X} \in \{\overline{B}, \overline{E}\}$, if $J \, X_{\mathbb{I}} \, I$ and $\mathcal{A}, J \models \psi$ for some $J \in \mathbb{I}$.

As an example, $\langle \mathrm{D} \rangle$ can be expressed in terms of $\langle \mathrm{B} \rangle$ and $\langle \mathrm{E} \rangle$ as $\langle \mathrm{D} \rangle \, \psi := \langle \mathrm{B} \rangle \, \langle \mathrm{E} \rangle \, \psi$, while $\langle \mathrm{A} \rangle$ can be expressed in terms of $\langle \mathrm{E} \rangle$ and $\langle \overline{\mathrm{B}} \rangle$ as $\langle \mathrm{A} \rangle \, \psi := ([\mathrm{E}] \, \bot \wedge (\psi \vee \langle \overline{\mathrm{B}} \rangle \, \psi)) \vee \langle \mathrm{E} \rangle ([\mathrm{E}] \, \bot \wedge (\psi \vee \langle \overline{\mathrm{B}} \rangle \, \psi))$.

State-based model-checking against HS. In the context of MC, finite state systems are usually modelled as finite Kripke structures over a finite set $\mathcal{AP}$ of atomic propositions which represent predicates over the states of the system.

▶ **Definition 2.** *A* Kripke structure *over $\mathcal{AP}$ is a tuple $\mathcal{K} = (\mathcal{AP}, S, E, Lab, s_0)$, where S is a set of states, $E \subseteq S \times S$ is a transition relation, $Lab : S \mapsto 2^{\mathcal{AP}}$ is a labelling function assigning to each state s the set of propositions that hold over it, and $s_0 \in S$ is the initial state. We say that $\mathcal{K}$ is finite if S is finite.*

Let $\mathcal{K} = (\mathcal{AP}, S, E, Lab, s_0)$ be a Kripke structure. A path π of $\mathcal{K}$ is a non-empty finite word over S such that for all $0 \leq i < |\pi|$, $(\pi(i), \pi(i+1)) \in E$. A *sub-path* (resp., *internal sub-path*) of π is a path of $\mathcal{K}$ which is a subword (resp., internal subword) of π. A path is *initial* if it starts from the initial state of $\mathcal{K}$.

We now recall the state-based approach [16] for model checking Kripke structures against HS formulas which consists in defining a mapping from a Kripke structure $\mathcal{K}$ to an AIM $\mathcal{A}_{\mathcal{K}}$, where the abstract intervals correspond to the paths of the Kripke structure, the relations $B_{\mathbb{I}}$ and $E_{\mathbb{I}}$ of $\mathcal{A}_{\mathcal{K}}$ are interpreted as the Allen's relations B and E over the set of $\mathcal{K}$-paths, respectively, and the following assumption is adopted: a proposition holds over an interval if and only if it holds over all its subintervals (*homogeneity principle*).

▶ **Definition 3.** *Let $\mathcal{K} = (\mathcal{AP}, S, E, Lab, s_0)$ be a Kripke structure. The AIM induced by $\mathcal{K}$ is $\mathcal{A}_{\mathcal{K}} = (\mathcal{AP}, \mathbb{I}, B_{\mathbb{I}}, E_{\mathbb{I}}, Lab_{\mathbb{I}})$, where $\mathbb{I}$ is the set of paths of $\mathcal{K}$, and:*

- $B_{\mathbb{I}} = \{(\pi, \pi') \in \mathbb{I} \times \mathbb{I} \mid \pi' \in \mathsf{Pref}(\pi)\}$, $E_{\mathbb{I}} = \{(\pi, \pi') \in \mathbb{I} \times \mathbb{I} \mid \pi' \in \mathsf{Suff}(\pi)\}$, *and*
- *for all $p \in \mathcal{AP}$, $Lab_{\mathbb{I}}^{-1}(p) = \{\pi \in \mathbb{I} \mid p \in \bigcap_{i=0}^{i<|\pi|} Lab(\pi(i))\}$.*

Note that for a finite Kripke structure $\mathcal{K}$, the number of paths in $\mathcal{K}$ may be infinite (this happens when $\mathcal{K}$ has loops), hence the number of intervals in $\mathcal{A}_\mathcal{K}$ may be infinite. A Kripke structure $\mathcal{K}$ over $\mathcal{AP}$ is a *model* of an HS formula ψ over $\mathcal{AP}$, written $\mathcal{K} \models \psi$, if for all *initial* paths π of $\mathcal{K}$, $\mathcal{A}_\mathcal{K}, \pi \models \psi$. In the following, we also write $\mathcal{K}, \pi \models \psi$ to mean $\mathcal{A}_\mathcal{K}, \pi \models \psi$. The (finite) model-checking problem (against HS) consists in checking whether $\mathcal{K} \models \psi$ for a given HS formula ψ and a finite Kripke structure $\mathcal{K}$.

We observe that the temporal modalities for the Allens's relations in $\{B, E, D\}$ have a "linear-time" semantics, i.e., they allow to select only slices (subpaths) of the current timeline (path). The semantics of the temporal modalities associated with the other Allen's relations (i.e., the ones in $\{A, L, O, \overline{A}, \overline{L}, \overline{B}, \overline{E}, \overline{D}, \overline{O}\}$) is instead "branching-time" (i.e., they allow to non-deterministically extend the current timeline in the future or in the past). Accordingly, a non-empty subset of non-interdefinable Allen's relations in $\{B, E, D\}$ is called a *linear-time basis* $\mathcal{B}$ of HS. Hence, the possible bases are $\{B\}$, $\{E\}$, $\{D\}$, $\{B, D\}$, $\{B, E\}$, and $\{E, D\}$.

3 Decision procedures based on descriptors

In this section, we provide a uniform framework for model-checking finite Kripke structures against the HS syntactical fragments, denoted by $\mathsf{HS}_\mathcal{B}(\mathcal{F})$, obtained by combining the modalities of a linear-time basis $\mathcal{B}$ of HS distinct from $\{D\}$ with the branching-time modalities for the Allen's relations in $\mathcal{F} = \{A, \overline{A}, \overline{B}, \overline{E}, L, \overline{L}\}$. Note that for the complete basis $\{B, E\}$, we obtain the full logic HS. Moreover, the Allen relation $\overline{D}$ can be expressed in terms of $\overline{B}$,$\overline{E}$: $\langle \overline{\mathrm{D}} \rangle \psi := \langle \overline{\mathrm{B}} \rangle \langle \overline{\mathrm{E}} \rangle \psi$. For the remaining branching-time modalities, i.e., the ones associated with O and $\overline{O}$, we have that $\langle \mathrm{O} \rangle$ (resp., $\langle \overline{\mathrm{O}} \rangle$) can be expressed in terms of $\langle \overline{\mathrm{B}} \rangle$ and $\langle \mathrm{E} \rangle$ (resp., $\langle \overline{\mathrm{E}} \rangle$ and $\langle \mathrm{B} \rangle$): $\langle \mathrm{O} \rangle \psi := \langle \mathrm{E} \rangle (\langle \mathrm{E} \rangle \top \wedge \langle \overline{\mathrm{B}} \rangle \psi)$ (resp., $\langle \overline{\mathrm{O}} \rangle \psi := \langle \mathrm{B} \rangle (\langle \mathrm{B} \rangle \top \wedge \langle \overline{\mathrm{E}} \rangle \psi)$). As an example, $\mathsf{HS}_{\{B\}}(\mathcal{F})$ corresponds to $\mathsf{A\overline{A}B\overline{B}D\overline{E}L\overline{L}O}$.

The proposed approach is a generalization of the one provided in [16], where only the full logic HS is considered. In particular, given a finite Kripke structure $\mathcal{K}$, for each linear-time basis $\mathcal{B}$ of HS, we define a finite abstraction of the set of $\mathcal{K}$-paths parameterized by a natural number h. This abstraction induces in turn a *finite* abstract interval model, which, in case $\mathcal{B} \neq \{D\}$, is equivalent to $\mathcal{A}_\mathcal{K}$ with respect to the fulfillment of all the formulas in $\mathsf{HS}_\mathcal{B}(\mathcal{F})$ having joint $\mathcal{B}$-nesting depth at most h. This allows us to provide in Subsection 3.1 an *alternating* algorithm, parameterized in the basis $\mathcal{B} \neq \{D\}$, for model-checking the fragment $\mathsf{HS}_\mathcal{B}(\mathcal{F})$, which given a finite Kripke structure $\mathcal{K}$ and a formula ψ, runs in time bounded by the size of the finite abstraction for the basis $\mathcal{B}$, the Kripke structure $\mathcal{K}$ and the parameter $h = \mathrm{depth}_\mathcal{B}(\psi)$, and whose number of alternations between existential and universal choices is at most $O(|\psi|)$. For each basis $\mathcal{B}$, we define in the following the notion of $\mathcal{B}$-*descriptor* which allows to construct the above mentioned finite abstraction. The definition of $\mathcal{B}$-*descriptors* exploits *h-level* Σ-*terms* and *h-level bipartite* Σ-*terms*, where Σ denotes a given finite alphabet and h a natural number. Intuitively, an h-level Σ-term corresponds to an unordered finite tree of height h such that subtrees rooted at distinct children of the same node are *not* isomorphic. An h-level bipartite Σ-term is similar but additionally we require that each edge in the tree has a color from a set of two colors. Formally, the set of h-level Σ-terms t is inductively defined as follows:

- if $h = 0$, then $t = a$ for some $a \in \Sigma$; otherwise, t has the form (a, T) where $a \in \Sigma$ and T is a (possibly empty) subset of $(h-1)$-level Σ-terms.

The set of h-level bipartite Σ-terms t is inductively defined as follows:

- if $h = 0$, then $t = a$ for some $a \in \Sigma$; otherwise t is of the form (a, T_1, T_2) where $a \in \Sigma$ and T_1 and T_2 are (possibly empty) subsets of $(h-1)$-level Σ-terms.

We say that a is the root of t. The size of an h-level (bipartite) Σ-term is the number of nodes in the associated tree representation. The following holds.

▶ Remark 4. The number of distinct h-level Σ-terms (resp., h-level bipartite Σ-terms) over Σ is $Tower(\Theta(|\Sigma|), h)$.

▶ **Definition 5** (Descriptors). *Let Σ be a finite alphabet and $\mathcal{B}$ be a linear-time basis of HS. Given a non-empty finite word w over Σ and $h \geq 0$, the h-level $\mathcal{B}$-descriptor $\mathcal{B}_h(w)$ of w is the h-level $(\Sigma \times 2^{\Sigma} \times \Sigma)$-term (resp., h-level bipartite $(\Sigma \times 2^{\Sigma} \times \Sigma)$-term) if $|\mathcal{B}| = 1$ (resp., $|\mathcal{B}| = 2$) inductively satisfying the following conditions. For the base case, i.e. $h = 0$, then $\mathcal{B}_0(w) = (\mathsf{fst}(w), \mathsf{internal}(w), \mathsf{lst}(w))$. For the induction step, i.e. $h > 0$, we have:*

- *Case $\mathcal{B} = \{B\}$ (resp., $\mathcal{B} = \{E\}$, resp., $\mathcal{B} = \{D\}$): $\mathcal{B}_h(w) = (\mathcal{B}_0(w), T)$ where T is the set of $(h-1)$-level $\mathcal{B}$-descriptors of the non-empty proper prefixes (resp., non-empty proper suffixes, resp., non-empty internal subwords) of w.*
- *Case $\mathcal{B} = \{B, E\}$: $\mathcal{B}_h(w) = (\mathcal{B}_0(w), T_B, T_E)$ with T_B (resp., T_E) the set of $(h-1)$-level $\mathcal{B}$-descriptors of the non-empty proper prefixes (resp., non-empty proper suffixes) of w.*
- *Case $\mathcal{B} = \{B, D\}$ (resp., $\mathcal{B} = \{E, D\}$): as in case $\mathcal{B} = \{B, E\}$ by replacing T_E (resp., T_B) with the set of $(h-1)$-level $\mathcal{B}$-descriptors of the non-empty internal subwords of w.*

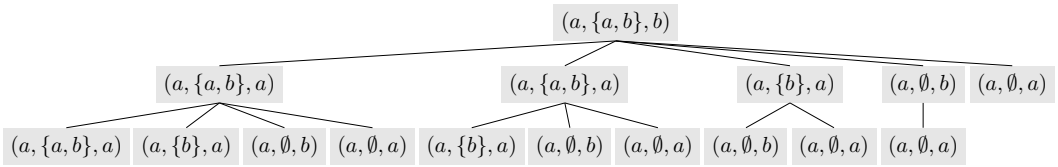


Figure 2 The 2-level $\{B\}$-descriptor for the word $w = abaaaab$ over $\Sigma = \{a, b\}$.

An example of 2-level $\{B\}$-descriptor is depicted in Figure 2. Intuitively, in case $\mathcal{B} \neq \{D\}$, the h-level $\mathcal{B}$-descriptor $\mathcal{B}_h(\pi)$ of a Kripke structure path π has enough information for checking the fulfillment of $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ formulas with joint $\mathcal{B}$-nesting depth at most h:

- for checking the fulfillment of proposition letters, $\mathcal{B}_h(\pi)$ keeps tracks at each node of the set of states visited by the *current subpath* of π;
- to deal with the branching-time modalities for the Allen's relations in $\mathcal{F}$, $\mathcal{B}_h(\pi)$ keeps tracks at each node also of the first and last states of the current subpath;
- finally, for checking the fulfillment of the linear-time modalities for the basis $\mathcal{B}$, $\mathcal{B}_h(\pi)$ keeps information about all the subpaths of the current subpath π' which can be obtained from π' by applying the Allen's relations in the basis $\mathcal{B}$.

For a basis $\mathcal{B} = \{X, Y\}$ (resp., $\mathcal{B} = \{X\}$), an h-level $\mathcal{B}$-descriptor is also called h-level XY-descriptor (resp., h-level X-descriptor) and for a non-empty word, we write $XY_h(w)$ (resp., $X_h(w)$) to mean $\mathcal{B}_h(w)$. For a finite Kripke structure $\mathcal{K}$, a basis $\mathcal{B}$, and $h \geq 0$, we denote by $\mathcal{B}_h(\mathcal{K})$ the finite set of h-level $\mathcal{B}$-descriptors associated with the paths of $\mathcal{K}$.

In the following we show that paths of $\mathcal{K}$ which have the same h-level $\mathcal{B}$-descriptor with $\mathcal{B} \neq \{D\}$ satisfy the same formulas in $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ whose joint $\mathcal{B}$-nesting depth is at most h. As a preliminary step, we show that the property of two paths π and π' to have the same h-level $\mathcal{B}$-descriptor is preserved by right (resp., left) $\star$-concatenation with another path of $\mathcal{K}$. This result is used for handling the branching-time modalities $\langle \overline{\mathrm{B}} \rangle$ and $\langle \overline{\mathrm{E}} \rangle$.

▶ **Proposition 6.** *Let $h \geq 0$, $\mathcal{B} \neq \{D\}$ a basis, and π and π' be two paths of a finite Kripke structure $\mathcal{K}$ having the same h-level $\mathcal{B}$-descriptor. Then, for all paths π_L and π_R of $\mathcal{K}$ such that $\pi_L \star \pi$ and $\pi \star \pi_R$ are defined, the following holds:*
(1) $\mathcal{B}_h(\pi \star \pi_R) = \mathcal{B}_h(\pi' \star \pi_R)$ and (2) $\mathcal{B}_h(\pi_L \star \pi) = \mathcal{B}_h(\pi_L \star \pi')$.

We note that Proposition 6 does not hold in general for the basis $\mathcal{B} = \{D\}$. As an example, let us consider a Kripke structure $\mathcal{K}$ consisting of three states s_1, s_2, and s_3 such that (s_i, s_j) is an edge of $\mathcal{K}$ for all $1 \leq i, j \leq 3$. Let us consider the two paths $\pi = s_1(s_2s_3)^3s_1$ and $\pi' = s_1(s_3s_2)^3s_1$. One can check that π and π' have the same 1-level D-descriptor. On the other hand, $\pi \cdot s_1$ and $\pi' \cdot s_1$ have distinct 1-level D-descriptors: in particular, while $\pi \cdot s_1$ has the internal subword s_3s_1, there is no internal subword ν' of $\pi' \cdot s_1$ such that $\mathsf{fst}(\nu') = s_3$, $\mathsf{lst}(\nu') = s_1$, and $\mathsf{internal}(\nu') = \emptyset$. By Proposition 6, we can obtain the following result.

▶ **Proposition 7.** *Let $h \geq 0$, $\mathcal{B} \neq \{D\}$ a basis, and π and π' be two paths of a finite Kripke structure $\mathcal{K}$ having the same h-level $\mathcal{B}$-descriptor. Then, for each $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ formula ψ with $\mathrm{depth}_{\mathcal{B}}(\psi) \leq h$, it holds that $\mathcal{K}, \pi \models \psi$ iff $\mathcal{K}, \pi' \models \psi$.*

By Proposition 6, for each basis $\mathcal{B} \neq \{D\}$, we can also state *a bounded path property* which intuitively provides a bounded witness for each $\mathcal{B}_h$-descriptor associated with an arbitrary path of a finite Kripke structure. The bounded path property will be crucial in Subsection 3.1 to design the MC algorithm for the logic $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$.

▶ **Proposition 8** (Bounded Path Property)**.** *Let $\mathcal{B} \neq \{D\}$ be a basis, $\mathcal{K}$ a finite Kripke structure, $h \geq 0$ and π a $\mathcal{K}$-path. Then, there exists a path π' having the same h-level $\mathcal{B}$-descriptor of π and whose length is bounded by $|\mathcal{B}_h(\mathcal{K})|$ (i.e., the number of distinct h-level $\mathcal{B}$-descriptors of the $\mathcal{K}$-paths).*

Proof. Let $|\pi| = n$. Since there are n distinct non-empty prefixes of π, if $n > |\mathcal{B}_h(\mathcal{K})|$, then π can be written in the form $\pi = \nu \cdot \nu' \cdot \nu''$ such that $|\nu| > 0$, $|\nu'| > 0$, and ν and $\nu \cdot \nu'$ have the same h-level $\mathcal{B}$-descriptor. By Proposition 6, the strictly smaller path $\nu \cdot \nu''$ has the same h-level $\mathcal{B}$-descriptor as π. We can iterate such a contraction process until there are no more pairs of prefixes with the same h-level $\mathcal{B}$-descriptor proving the statement. ◀

By Propositions 7 and 8 we can define bounded minimal representatives ($\mathcal{B}$-certificates) of paths used in the MC algorithm defined in the next section.

▶ **Definition 9** ($\mathcal{B}$-certificate)**.** *Given a basis $\mathcal{B} \neq \{D\}$, a finite Kripke structure $\mathcal{K}$, and $h \geq 0$, an* h-level $\mathcal{B}$-certificate of $\mathcal{K}$ *is a path π of $\mathcal{K}$ such that there is no path π' so that $|\pi'| < |\pi|$ and π and π' have the same h-level $\mathcal{B}$-descriptor. Given an $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ formula φ, a* $\mathcal{B}$-certificate for $(\mathcal{K}, \varphi)$ *is an h-level $\mathcal{B}$-certificate of $\mathcal{K}$ where $h = \mathrm{depth}_{\mathcal{B}}(\varphi)$.*

By Proposition 8 an upper bound on the length of $\mathcal{B}$-certificates for $(\mathcal{K}, \varphi)$ is $|\mathcal{B}_h(\mathcal{K})|$ with $h = \mathrm{depth}_{\mathcal{B}}(\varphi)$.

3.1 Algorithm for model-checking the logics $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$

In this section, by exploiting Propositions 6–8, for each basis $\mathcal{B} \neq \{D\}$, we provide an alternating MC algorithm for the logic $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ (recall that $\mathcal{F} = \{A, \overline{A}, \overline{B}, \overline{E}, L, \overline{L}\}$). We assume that $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ formulas are in *PNF*. As complexity measures of a formula φ, we consider the size $|\varphi|$ and the standard *alternation depth*, denoted by $\Upsilon(\varphi)$, between the existential $\langle \mathrm{X} \rangle$ and universal modalities $[\mathrm{X}]$ occurring in the *PNF* of φ for $X \in \{\overline{B}, \overline{E}\}$. Formally, we establish the following result, where $\mathsf{MC}_{\mathcal{B}}$ is the set of pairs $(\mathcal{K}, \varphi)$ consisting of a finite Kripke structure $\mathcal{K}$ and a $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ formula φ such that $\mathcal{K} \models \varphi$.

▶ **Theorem 10.** *For each basis $\mathcal{B} \neq \{D\}$, one can construct a time-bounded Alternating Turing Machine (ATM) accepting $\mathsf{MC}_{\mathcal{B}}$ which, given an input $(\mathcal{K}, \varphi)$, has a number of alternations (between existentially and universal choices) at most $\Upsilon(\varphi) + 2$ and runs in time $M_{\mathcal{B}}(\mathcal{K}, \varphi)^{O(|\varphi|^d)}$, where $M_{\mathcal{B}}(\mathcal{K}, \varphi)$ is the maximal length of a $\mathcal{B}$-certificate for the input, and $d = 2$ if $D \in \mathcal{B}$ and $d = 1$ otherwise.*

check$_{\mathcal{B}}(\mathcal{K},\varphi)$ [$\mathcal{K}$ *is a finite Kripke structure and* φ *is an* $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ *formula in PNF*]

---

existentially choose an $\mathsf{A\overline{A}L\overline{L}}$-labeling $\mathcal{L}$ for $(\mathcal{K},\varphi)$;
for each state s and $\psi \in \mathcal{L}(s)$ **do**
  case $\psi = \langle \mathrm{A}\rangle\,\psi'$ (resp., $\psi = [\mathrm{A}]\,\psi'$): **existentially** (resp., **universally**) **choose** a $\mathcal{B}$-certificate π with $\mathsf{fst}(\pi) = s$ and **call** *checkTrue*$_{\mathcal{B}}(\mathcal{K},\varphi,\mathcal{L},\{(\psi',\pi)\})$;
  case $\psi = \langle \overline{\mathrm{A}}\rangle\,\psi'$ (resp., $\psi = [\overline{\mathrm{A}}]\,\psi'$): **existentially** (resp., **universally**) **choose** a $\mathcal{B}$-certificate π with $\mathsf{lst}(\pi) = s$ and **call** *checkTrue*$_{\mathcal{B}}(\mathcal{K},\varphi,\mathcal{L},\{(\psi',\pi)\})$;
  case $\psi = \langle \mathrm{L}\rangle\,\psi'$ (resp., $\psi = [\mathrm{L}]\,\psi'$): **existentially** (resp., **universally**) **choose** state s' s.t. $s \rightarrow_{\mathcal{K}}^{+} s'$ and a $\mathcal{B}$-certificate π with $\mathsf{fst}(\pi) = s'$ and **call** *checkTrue*$_{\mathcal{B}}(\mathcal{K},\varphi,\mathcal{L},\{(\psi',\pi)\})$;
  case $\psi = \langle \overline{\mathrm{L}}\rangle\,\psi'$ (resp., $\psi = [\overline{\mathrm{L}}]\,\psi'$): **existentially** (resp., **universally**) **choose** state s' s.t. $s' \rightarrow_{\mathcal{K}}^{+} s$ and a $\mathcal{B}$-certificate π with $\mathsf{lst}(\pi) = s'$ and **call** *checkTrue*$_{\mathcal{B}}(\mathcal{K},\varphi,\mathcal{L},\{(\psi',\pi)\})$;
universally choose a certificate π for $(\mathcal{K},\varphi)$ with $\mathsf{fst}(\pi) = s_0$ (s_0 is the initial state of $\mathcal{K}$)
  and **call** *checkTrue*$_{\mathcal{B}}(\mathcal{K},\varphi,\mathcal{L},\{(\varphi,\pi)\})$;

Figure 3 Procedure *check*$_{\mathcal{B}}$ for a linear-time basis $\mathcal{B} \neq \{D\}$.

To prove the assertion of Theorem 10 we define a procedure, parametric in the basis $\mathcal{B} \neq \{D\}$, which can be easily translated into an ATM. To this end, we introduce some auxiliary notation. Let us fix a finite Kripke structure $\mathcal{K}$ and an $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ formula φ in *PNF*. For two states s and s', we write $s \rightarrow_{\mathcal{K}}^{+} s'$ to mean that s' is reachable from s by a path of length at least 2. Let π be a $\mathcal{B}$-certificate for $(\mathcal{K},\varphi)$ and $h = \mathrm{depth}_{\mathcal{B}}(\varphi)$. For each $X \in \mathcal{B}$, an X-witness of π is a non-empty proper prefix (resp., non-empty proper suffix, resp., non-empty internal subpath) of π if $X = B$ (resp., $X = E$, resp., $X = D$). A $\overline{B}$-*witness* (resp., $\overline{E}$-*witness*) of π for $(\mathcal{K},\varphi)$, is a $\mathcal{B}$-certificate π' of $(\mathcal{K},\varphi)$ such that π' has the same h-level $\mathcal{B}$ descriptor of a path of the form $\pi \star \pi''$ (resp., $\pi'' \star \pi$) for some $\mathcal{B}$-*certificate* π'' of $(\mathcal{K},\varphi)$ with $|\pi''| > 1$. By $\mathsf{SD}(\varphi)$ we denote the set consisting of the subformulas ψ of φ and the *duals* $\widetilde{\psi}$. By Propositions 6–8, we easily deduce the following property.

▶ **Proposition 11.** *Let* $\mathcal{B} \neq \{D\}$ *be a basis,* φ *an* $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ *formula in PNF,* $\mathcal{K}$ *a finite Kripke structure, and* π *a* $\mathcal{B}$*-certificate for* $(\mathcal{K},\varphi)$*. Then, for each* $\langle \mathrm{X}\rangle\,\psi \in \mathsf{SD}(\varphi)$ *with* $X \in \{\overline{B},\overline{E}\}$, $\mathcal{K},\pi \models \langle \mathrm{X}\rangle\,\psi$ *iff there is an* X*-witness* π' *of* π *for* $(\mathcal{K},\varphi)$ *such that* $\mathcal{K},\pi' \models \psi$.

The set $\mathsf{A\overline{A}L\overline{L}}(\varphi)$ is the set of formulas in $\mathsf{SD}(\varphi)$ of the form $\langle \mathrm{X}\rangle\,\psi'$ or $[\mathrm{X}]\,\psi'$ with $X \in \{A,\overline{A},L,\overline{L}\}$. An $\mathsf{A\overline{A}L\overline{L}}$-labeling $\mathcal{L}$ for $(\mathcal{K},\varphi)$ is a mapping associating with each state s of $\mathcal{K}$ a maximally consistent set of subformulas of $\mathsf{A\overline{A}L\overline{L}}(\varphi)$. More precisely, for all $s \in S$, $\mathcal{L}(s)$ is such that for all $\psi, \widetilde{\psi} \in \mathsf{A\overline{A}L\overline{L}}(\varphi)$, $\mathcal{L}(s) \cap \{\psi,\widetilde{\psi}\}$ is a singleton. $\mathcal{L}$ is *valid* if for all states $s \in S$ and $\psi \in \mathcal{L}(s)$, $\mathcal{K},s \models \psi$ (we consider s as a length-1 path). Finally, a *well-formed set for* $(\mathcal{K},\varphi)$ is a finite set $\mathcal{W}$ consisting of pairs (ψ,π) such that $\psi \in \mathsf{SD}(\varphi)$ and π is a $\mathcal{B}$-certificate of $(\mathcal{K},\varphi)$. $\mathcal{W}$ is said *universal* if each formula occurring in $\mathcal{W}$ is of the form $[\mathrm{X}]\,\psi$ with $X \in \{\overline{B},\overline{E}\}$. The *dual* $\widetilde{\mathcal{W}}$ of $\mathcal{W}$ is the well-formed set obtained by replacing each pair $(\psi,\pi) \in \mathcal{W}$ with $(\widetilde{\psi},\pi)$. A well-formed set $\mathcal{W}$ is *valid* if for each $(\psi,\pi) \in \mathcal{W}$, $\mathcal{K},\pi \models \psi$.

The procedure *check*$_{\mathcal{B}}$ in Figure 3 defines the ATM required to prove the assertion of Theorem 10 for a basis $\mathcal{B} \neq \{D\}$. It takes a pair $(\mathcal{K},\varphi)$ as input, where φ is an $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ formula, and: (1) it guesses an $\mathsf{A\overline{A}L\overline{L}}$-labeling $\mathcal{L}$ for $(\mathcal{K},\varphi)$; (2) it checks that the guessed labeling $\mathcal{L}$ is valid; (3) for every $\mathcal{B}$-certificate π of $(\mathcal{K},\varphi)$ starting from the initial state, it checks that $\mathcal{K},\pi \models \varphi$. To perform steps (2)–(3), it exploits the auxiliary ATM procedure *checkTrue*$_{\mathcal{B}}$ reported in Figure 4. The procedure *checkTrue*$_{\mathcal{B}}$ takes as input a well-formed set $\mathcal{W}$ for $(\mathcal{K},\varphi)$ and, assuming that the current $\mathsf{A\overline{A}L\overline{L}}$-labeling $\mathcal{L}$ is valid, checks whether $\mathcal{W}$ is valid. For each pair $(\psi,\pi) \in \mathcal{W}$ such that ψ is not of the form $[\mathrm{X}]\,\psi'$ with $X \in \{\overline{B},\overline{E}\}$,

checkTrue$_{\mathcal{B}}(\mathcal{K}, \varphi, \mathcal{L}, \mathcal{W})$ [$\mathcal{W}$ *is a well-formed set and* $\mathcal{L}$ *is an* $\mathsf{A\overline{A}L\overline{L}}$*-labeling for* $(\mathcal{K}, \Phi)$]

---

while $\mathcal{W}$ is *not* universal **do**
  deterministically select $(\psi, \pi) \in \mathcal{W}$ such that ψ is not of the form $[\overline{E}]\psi'$ and $[\overline{B}]\psi'$
  update $\mathcal{W} \leftarrow \mathcal{W} \setminus \{(\psi, \pi)\}$;
  case $\psi = p$ (resp., $\psi = \neg p$) with $p \in \mathcal{AP}$: **if** $\mathcal{K}, \pi \not\models p$ (resp., $\mathcal{K}, \pi \not\models \neg p$) **then** *reject*;
  case $\psi = \langle \mathrm{X} \rangle \psi'$ or $\psi = [\mathrm{X}]\psi'$ with $X \in \{A, L\}$: **if** $\psi \notin \mathcal{L}(\mathsf{lst}(\pi))$ **then** *reject*;
  case $\psi = \langle \mathrm{X} \rangle \psi'$ or $\psi = [\mathrm{X}]\psi'$ with $X \in \{\overline{A}, \overline{L}\}$: **if** $\psi \notin \mathcal{L}(\mathsf{fst}(\pi))$ **then** *reject*;
  case $\psi = \psi_1 \vee \psi_2$: **existentially choose** $i = 1, 2$, **update** $\mathcal{W} \leftarrow \mathcal{W} \cup \{(\psi_i, \pi)\}$;
  case $\psi = \psi_1 \wedge \psi_2$: **update** $\mathcal{W} \leftarrow \mathcal{W} \cup \{(\psi_1, \pi), (\psi_2, \pi)\}$;
  case $\psi = [\mathrm{X}]\psi'$ with $X \in \mathcal{B}$: **update** $\mathcal{W} \leftarrow \mathcal{W} \cup \{(\psi', \pi') \mid \pi'$ is an X*-witness* of $\pi\}$;
  case $\psi = \langle \mathrm{X} \rangle \psi'$ with $X \in \mathcal{B} \cup \{\overline{E}, \overline{B}\}$: **existentially choose** an X*-witness* π' of π for $(\mathcal{K}, \varphi)$, **update** $\mathcal{W} \leftarrow \mathcal{W} \cup \{(\psi', \pi')\}$;
end while
if $\mathcal{W} = \emptyset$ **then** *accept*
else universally choose $(\psi, \pi) \in \widetilde{\mathcal{W}}$ and **call** *checkFalse*$_{\mathcal{B}}(\mathcal{K}, \varphi, \mathcal{L}, \{(\psi, \rho)\})$

Figure 4 Procedure *checkTrue*$_{\mathcal{B}}$ for a linear-time basis $\mathcal{B} \neq \{D\}$.

checkTrue$_{\mathcal{B}}$ directly checks whether $\mathcal{K}, \pi \models \psi$. In order to allow a deterministic choice of the current element of the iteration, we assume that the set $\mathcal{W}$ is implemented as an ordered data structure. At each iteration of the while loop in *checkTrue*$_{\mathcal{B}}$, the current pair $(\psi, \pi) \in \mathcal{W}$ is processed according to the semantics of HS, exploiting the guessed $\mathsf{A\overline{A}L\overline{L}}$-labeling $\mathcal{L}$ and Proposition 11. The processing is either deterministic or based on an existential choice, and the currently processed pair (ψ, π) is either removed from $\mathcal{W}$, or replaced with pairs (ψ', π') such that ψ' is a strict subformula of ψ.

At the end of the while loop, the resulting well formed set $\mathcal{W}$ is either empty or universal. In the former case, the procedure accepts. In the latter case, there is a switch in the current operation mode. For each element (ψ, π) in the dual of $\mathcal{W}$ (note that the root modality of ψ is either $\langle \overline{\mathrm{E}} \rangle$ or $\langle \overline{\mathrm{B}} \rangle$), the auxiliary ATM procedure *checkFalse*$_{\mathcal{B}}$ is invoked, which accepts the input $\{(\psi, \pi)\}$ iff $\mathcal{K}, \pi \not\models \psi$. The procedure *checkFalse*$_{\mathcal{B}}$ is the *dual* of *checkTrue*$_{\mathcal{B}}$: it is simply obtained from *checkTrue*$_{\mathcal{B}}$ by switching *accept* and *reject*, by switching existential choices and universal choices, and by converting the last call to *checkFalse*$_{\mathcal{B}}$ into *checkTrue*$_{\mathcal{B}}$. Thus *checkFalse*$_{\mathcal{B}}$ accepts an input $\mathcal{W}$ iff $\mathcal{W}$ is *not* valid.

Note that the number of alternations of the ATM *check*$_{\mathcal{B}}$ between existential and universal choices is the number of switches between the calls to the procedures *checkTrue*$_{\mathcal{B}}$ and *checkFalse*$_{\mathcal{B}}$ plus two. The correctness of the algorithm follows from Propositions 7, 8 and 11.

4 Tight bounds on the length of certificates

In this section, for each basis $\mathcal{B}$ (except $\{D\}$), we provide tight bounds on the length of h-level $\mathcal{B}$-certificates. For the bases $\{B\}$ and $\{E\}$ (see Subsection 4.1), we prove singly exponential upper bounds and matching lower bounds. By Theorem 10, we deduce that model-checking the logics $\mathsf{HS}_{\{B\}}(\mathcal{F})$ and $\mathsf{HS}_{\{E\}}(\mathcal{F})$ is in the complexity class $\mathbf{AEXP_{pol}}$ of problems decided by exponential-time bounded alternating Turing Machines with a polynomially bounded number of alternations. On the other hand, for all bases $\mathcal{B}$ distinct from $\{B\}$ and $\{E\}$, we state a non-elementary lower bound (see Subsection 4.2). In particular, the result obtained for the basis $\{B, E\}$ negatively answers a question left open in [16] regarding the possibility of fixing an elementary upper bound on the size of BE-descriptors.

4.1 Tight bounds on the length of B-certificates and E-certificates

In this section, we provide exponential upper bounds and exponential lower bounds on the length of h-level B-certificates and E-certificates of a finite Kripke structure.

▶ **Theorem 12.** *The following holds:*

- Upper bound: *let $\mathcal{K}$ be a finite Kripke structure with set of states S and $h \geq 0$. Then, each h-level B-certificate (resp., h-level E-certificate) has length at most $|S|^{2h+2}$.*
- Lower bound: *there is a family $\{\mathcal{K}_n\}_{n\geq 1}$ of finite Kripke structures such that for all $n \geq 1$, $\mathcal{K}_n$ has $O(n)$ states and for all $h \geq 1$, there are h-level B-certificates (resp., h-level E-certificates) of $\mathcal{K}_n$ whose length is at least $\frac{1}{h+1} \cdot (\frac{n}{h+1})^{h+1} \cdot e^h$.*

By Theorem 10 and the upper bound in Theorem 12, and considering that model-checking $\overline{\mathsf{B}}$ and $\overline{\mathsf{E}}$ is already **PSPACE**-hard, we obtain the following result.

▶ **Corollary 13.** *For the basis $\mathcal{B} = \{B\}$ (resp., $\mathcal{B} = \{E\}$), model-checking the logic $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ is in $\mathbf{AEXP_{pol}}$ and at least* **PSPACE***-hard.*

Considering that $\mathbf{AEXP_{pol}} \subseteq \mathbf{EXPSPACE}$, our result improves the **EXPSPACE** upper-bounds for the smaller fragments $\mathsf{A\overline{A}B\overline{B}E}$ and $\mathsf{A\overline{A}E\overline{B}E}$ obtained in [17] by a much more involved technique. In the following, we prove Theorem 12 focusing on B-certificates (the proof for E-certificates is similar and omitted).

Upper bound in Theorem 12 for B-certificates. In order to prove Theorem 12(1), for a given finite alphabet Σ and $h \geq 0$, we first define a variant of the notion of h-level B-descriptor, called *ordered h-prefix descriptor over Σ*, which is not related to a specific word over Σ. The set OPD_h of ordered h-prefix descriptors over Σ is partitioned into $|\Sigma|$ subsets OPD_h^b (for each $b \in \Sigma$), where each of them is equipped with a strict partial order. We show that (i) each strict ascendent chain of elements in OPD_h^b has length at most $O(|\Sigma|^{2h+1})$, (ii) the h-level B-descriptor of a word $w \in \Sigma^+$ is an element in OPD_h, and (iii) for each $w \in \Sigma^+$, the h-level B-descriptors associated to the prefixes of w can be grouped into at most $|\Sigma|$ non-strict ascendent chains. Thus, by Proposition 6 and reasoning as in Proposition 8, we fix the upper bound on the length of h-level B-certificates for a given finite Kripke structure.

Let $h \geq 0$. For a $(\Sigma \times 2^\Sigma \times \Sigma)$-term t with root (a, I, b), we say that a (resp., b) is the *first symbol* (resp., *last symbol*) of t.

▶ **Definition 14** (Ordered prefix descriptors). *Let Σ be a finite alphabet and $h \geq 0$. We define by induction on h a pair $(OPD_h, \prec_h)$ consisting of a set OPD_h of h-level $(\Sigma \times 2^\Sigma \times \Sigma)$-terms, called* ordered h-prefix descriptors over Σ *and a binary relation $\prec_h$ over OPD_h.*

- *$h = 0$: OPD_0 coincides with the set of 0-level $(\Sigma \times 2^\Sigma \times \Sigma)$-terms. Given (a, I, b), $(a', I', b') \in OPD_0$, $(a, I, b) \prec_0 (a', I', b')$ if (i) $a = a'$ (equality between the initial symbols) and (ii) $I \cup \{b\} \subseteq I' \cup \{b'\}$, and either $b \neq b'$ or $I \cup \{b\} \subset I' \cup \{b'\}$.*
- *$h > 0$: OPD_h is the set of h-level $(\Sigma \times 2^\Sigma \times \Sigma)$-terms $t = ((a, I, b), T)$ such that T is a (possibly empty) set of the form $T = \{t_1, \ldots, t_n\}$ where $t_i \in OPD_{h-1}$, t_i has initial symbol a, and $t_i \prec_{h-1} t_j$ for all $i \in [1, n]$ and $j \in [i + 1, n]$. The binary relation $\prec_h$ is defined as follows: $((a, I, b), T) \prec_h ((a', I', b'), T')$ if*
  - *$a = a'$, $I \cup \{b\} \subseteq I' \cup \{b'\}$, $T \subseteq T'$;*
  - either $b \neq b'$ or $I \cup \{b\} \subset I' \cup \{b'\}$ or $T \subset T'$.

By construction for each $b \in \Sigma$, the binary relation $\prec_h$ is a strict partial order over the set OPD_h^b of ordered h-prefix descriptors over Σ having the same last symbol b. Additionally, we show that a strict ascendent chain of elements in OPD_h^b has length at most $|\Sigma|^{2h+1}$.

▶ **Proposition 15.** *Let $h \geq 0$, Σ be a finite alphabet, $b \in \Sigma$, and $t_1, \ldots, t_n$ be ordered h-prefix descriptors having last symbol b such that $t_1 \prec_h t_2 \prec_h \ldots \prec_h t_n$. Then, $n \leq |\Sigma|^{2h+1}$.*

Proof. The proof is by induction on $h \geq 0$. For $h = 0$, there is $a \in \Sigma$ s.t. for all $i \in [1, n]$, $t_i = (a, I_i, b)$ for some $I_i \subseteq \Sigma$, and $I_1 \subset I_2 \subset \ldots \subset I_n$. Hence, $n \leq |\Sigma|$ and the result follows.

Now, let $h > 0$. Hence, there is $a \in \Sigma$ s.t. for all $i \in [1, n]$, t_i is of the form $t_i = ((a, I_i, b), T_i)$. By hypothesis, $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n$. Moreover, for each $i \in [1, n]$, T_i can be partitioned into at most $|\Sigma|$ strict ascendent chains of ordered $h-1$-prefix descriptors having the same last symbol. Thus, by the induction hypothesis, we have that $|T_i| \leq |\Sigma| \cdot |\Sigma|^{2(h-1)+1} = |\Sigma|^{2h}$ for all $i \in [1, n]$. Fix an arbitrary $i \in [1, n]$. We claim that for each $j \in [i, n]$ such that $I_j = I_i$, it holds that $|j - i| \leq |\Sigma|^{2h}$. Hence, evidently, the result follows. Fix $i, j \in [1, n]$ such that $i < j$ and $I_j = I_i$. Since $t_i \prec_h t_\ell$ for all $\ell \in [i+1, j]$, we have that $|T_i| < |T_{i+1}| < \ldots < |T_j|$. Hence, $j - i \leq |T_j|$ and since $|T_j| \leq |\Sigma|^{2h}$, the result follows. ◀

By exploiting Proposition 15, we deduce the following proposition, from which the upper bound for the h-level B-certificates in Theorem 12 directly follows.

▶ **Proposition 16.** *Let $\mathcal{K}$ be a finite Kripke structure with set of states S, $h \geq 0$, and π a path of $\mathcal{K}$. Then, the following holds:*

1. *for all $i, j \in [0, n]$ where $n = |\pi| - 1$, (i) $B_h(\pi[0, i])$ is an ordered h-prefix descriptor, and (ii) if $j \in [i+1, n]$ and $B_h(\pi[0, i]) \neq B_h(\pi[0, j])$, then $B_h(\pi[0, i]) \prec_h B_h(\pi[0, j])$;*
2. *there is a path π' having the same h-level B-descriptor as π s.t. $|\pi'|$ is at most $|S|^{2h+2}$.*

Proof. Property 1 can be proved by a straightforward induction on $h \geq 0$. Now, let us consider Property 2. By reasoning as in the proof of Proposition 8, there is a path π' of $\mathcal{K}$ having the same h-level B-descriptor as π and such that distinct non-empty prefixes of π' have distinct h-level B-descriptors as well. Let s be a state visited by π', then by Property 1, the set of h-level B-descriptors associated with the non-empty prefixes of π' ending at state s form a strict ascending chain (with respect $\prec_h$) whose length n_s coincides with the set of positions i of π' such that $\pi'(i) = s$. By Proposition 15, $n_s \leq |S|^{2h+1}$. Since $|\pi'| = \sum_{s \in S(\pi')} n_s$ where $S(\pi')$ is the set of states visited by π', we obtain that $|\pi'| \leq |S|^{2h+2}$. ◀

Lower bound in Theorem 12 for B-certificates. For each $n \geq 1$, let $\Sigma_n = \{a_1, \ldots, a_n\}$ be an alphabet consisting of n distinct symbols a_1, ..., a_n. We exhibit a family $(w_n^h)_{h \geq 0}$ of non-empty words over Σ_n such that for each $h \geq 0$, the length of w_n^h is at least $\frac{1}{h+1} \cdot (\frac{n}{h+1})^{h+1} \cdot e^h$ and w_n^h is a minimal representative of the $h+1$-level B-descriptor $B_{h+1}(w_n^h)$.

Fix $n \geq 1$. Formally, for all $i, j \in [1, n]$ and $h \geq 0$, we define by induction on $h \geq 0$, a non-empty word $w_{i,j,h}$ over Σ_n called (i, j, h)-*miniword*:

1. Case $h = 0$: if $i \leq j$, then $w_{i,j,h} = a_i a_{i+1} \ldots a_j$. Otherwise, $w = a_j a_{j-1} \ldots a_i$. The set of *main positions* of $w_{i,j,h}$ is the set of all its positions.
2. Case $h > 0$: if $i \leq j$, then $w_{i,j,h} = a_i \cdot w_i \cdot a_{i+1} \cdot w_{i+1} \cdot \ldots \cdot a_j \cdot w_j$ where for each $\ell \in [i, j]$, w_ℓ is the $(\ell, i, h-1)$-miniword. Otherwise, $w_{i,j,h} = a_i \cdot u_i \cdot a_{i-1} \cdot u_{i-1} \cdot \ldots \cdot a_j \cdot u_j$ where for each $\ell \in [j, i]$, u_ℓ is the $(\ell, i, h-1)$-miniword. The subwords w_ℓ (resp., u_ℓ) with $\ell \in [i, j]$ (resp., $\ell \in [j, i]$) are called *secondary subwords* of $w_{i,j,h}$, while a *main position* of $w_{i,j,h}$ is a position which is not associated to a secondary-subword position.

We say that $w_{i,j,h}$ *has level* h. Note that by construction, for each symbol a occurring in $w_{i,j,h}$, the smallest position ℓ such that $w_{i,j,h}(\ell) = a$ is a main position. We can show that distinct prefixes of h-level miniwords have distinct h-level B-descriptors as well.

▶ **Proposition 17.** *Let $n \geq 1$ and $h \geq 0$. Then, for each miniword w over Σ_n of level h, distinct prefixes of w have distinct h-level B-descriptors.*

For $\Sigma_n = \{a_1, \ldots, a_n\}$, let $K(\Sigma_n)$ be the Kripke structure $(\Sigma_n, \Sigma_n, E, Lab, a_1)$, where Lab is the identity and $(a_i, a_j) \in E$ for all $i, j \in [1, n]$. The set of paths in $K(\Sigma_n)$ is the set of non-empty finite words over Σ_n. Hence, the lower bound in Theorem 12 for B-certificates directly follows from the following result which is obtained by exploiting Proposition 17.

▶ **Proposition 18.** *Let $n \geq 1$, $i, j \in [1, n]$, and $h \geq 0$. For the (i, j, h) miniword $w_{i,j,h}$ over Σ_n, the length of $w_{i,j,h}$ is at least $\frac{1}{h+1} \cdot (\frac{|i-j|+1}{h+1})^{h+1} \cdot e^h$ and there is no smaller word u over Σ_n (i.e., such that $|u| < |w_{i,j,h}|$) having the same $h+1$-level B-descriptor as $w_{i,j,h}$.*

Proof. For the (i, j, k) miniword $w_{i,j,h}$, let $p = |i - j| + 1$. By construction, the length of $w_{i,j,h}$, denoted by $L(p, h)$, depends only on h and p, and satisfies the recurrence: $L(p, h) = p$ if $h = 0$, and $L(p, h) = p + \sum_{\ell=1}^{\ell=p} L(\ell, h-1)$ otherwise. We first show by induction on $h \geq 0$ that $L(p, h) \geq \frac{p^{h+1}}{(h+1)!}$. The base case ($h = 0$) is obvious. Now, let $h > 0$. By the induction hypothesis and the fact that $\sum_{\ell=1}^{\ell=p} \ell^h \geq \frac{p^{h+1}}{h+1}$ (Faulhaber's formula), we have that $L(p, h) = p + \sum_{\ell=1}^{\ell=p} L(\ell, h-1) \geq \sum_{\ell=1}^{\ell=p} \frac{\ell^h}{h!} \geq \frac{p^{h+1}}{(h+1)!}$. Thus, since $(h+1)! \leq \frac{(h+1)^{h+2}}{e^h}$, the claimed lower bound follows. Now, let T be the set of h-level B-descriptors of the non-empty proper prefixes of $w_{i,j,h}$, and u a non-empty word having the same $h+1$-level B-descriptor as $w_{i,j,h}$. Since the number of non-empty proper prefixes of a non-empty word w is $|w| - 1$, by hypothesis, we have that $|u| - 1 \geq |T|$. On the other hand, by Proposition 17, $|w_{i,j,h}| - 1 = |T|$. Hence, $|u| \geq |w_{i,j,h}|$, which concludes the proof of Proposition 18. ◀

4.2 Non-elementary lower bounds on the length of BD-certificates, BE-certificates, and ED-certificates

In this section, for each linear-time basis $\mathcal{B} \in \{\{B, D\}, \{B, E\}, \{E, D\}\}$, we establish a non-elementary lower bound on the length of h-level $\mathcal{B}$-certificates. Hence, in particular, we obtain a non-elementary lower bound on the running time of the algorithm for model-checking the logic $\mathsf{HS}_{\mathcal{B}}(\mathcal{F})$ presented in Section 3.1.

▶ **Theorem 19.** *There is a family $\{\mathcal{K}_n\}_{n \geq 1}$ of finite Kripke structures such that for all $n \geq 1$, $\mathcal{K}_n$ has $O(n)$ states and for all $k \in [0, n-1]$ and basis $\mathcal{B}$ with $\mathcal{B} \in \{\{B, D\}, \{E, D\}\}$ (resp., $\mathcal{B} = \{B, E\}$), there are k-level (resp., $2k$-level) $\mathcal{B}$-certificates of $\mathcal{K}_n$ having length at least $\Omega(Tower(n, k+1))$.*

In the rest of this section we provide a proof of Theorem 19. We first show as an intermediate and crucial step that there is a family $\{\Sigma_n\}_{n \geq 1}$ of finite alphabets such that for all $n \geq 1$, Σ_n has cardinality $O(n)$ and for all $h \in [0, n-1]$, there are $\Omega(Tower(n, h+1))$ words over Σ_n having pairwise distinct h-level D-descriptors (resp., $2h$-level BE-descriptors).

Fix $n \geq 1$ and let Σ_n be the finite alphabet having cardinality $O(n)$ given by

$$\Sigma_n = \bigcup_{i \in [2,n]} \{\$_i\} \cup \bigcup_{bit \in \{0,1\}} \bigcup_{i \in [1,n]} \{(\$_i, bit)\} \cup \bigcup_{bit \in \{0,1\}} \bigcup_{i \in [1,n]} \{(i, bit)\}$$

Moreover, for each $h \in [1, n]$, let Σ_n^h be the subset of Σ_n given by

$$\Sigma_n^h = \Sigma_n \setminus \Big(\bigcup_{i \in [h+1,n]} \{\$_i\} \cup \bigcup_{bit \in \{0,1\}} \bigcup_{i \in [h+1,n]} \{(\$_i, bit)\} \Big)$$

For each $h \in [1, n]$, we define a suitable encoding of the natural numbers in $[0, \mathit{Tower}(n, h)-1]$ by finite words over Σ_n^h, called (n, h)-*blocks*. In particular, for $h > 1$, a (n, h)-block encoding a natural number $m \in [0, \mathit{Tower}(n, h) - 1]$ is a sequence of $\mathit{Tower}(n, h - 1)$ $(n, h - 1)$-blocks, where the i^{th} $(n, h - 1)$-block encodes both the value and (recursively) the position of the i^{th}-bit in the binary representation of m. Formally, the set of (n, h)-blocks is defined by induction on h as follows:

Base Step: $h = 1$. A $(n, 1)$-block is a finite word bl over Σ_n^1 of length $n+2$ having the form $bl = (\$_1, bit)(1, bit_1) \dots (n, bit_n)(\$_1, bit)$ such that $bit, bit_1, \dots, bit_n \in \{0, 1\}$. The *content* of bl is bit, and the *index* of bl is the natural number in $[0, \mathit{Tower}(n, 1) - 1]$ (recall that $\mathit{Tower}(n, 1) = 2^n$) whose binary code is $bit_1 \dots bit_n$.

Induction Step: $1 < h \leq n$. A (n, h)-*block* is a finite word bl over Σ_n^h having the form $(\$_h, bit) \cdot bl_0 \cdot \$_h \cdot \ldots \cdot bl_{\ell-1} \cdot \$_h \cdot bl_\ell \cdot (\$_h, bit)$ such that $\ell = \mathit{Tower}(n, h - 1) - 1$, $bit \in \{0, 1\}$ and for all $i \in [0, \ell]$, bl_i is a $(n, h - 1)$-block having index i. The *content* of bl is bit and the *index* of bl is the natural number in $[0, \mathit{Tower}(n, h) - 1]$ whose binary code is given by $bit_0, \dots, bit_\ell$, where bit_i is the content of the sub-block bl_i for all $0 \leq i \leq \ell$.

By construction, the following holds.

▶ Remark 20. For all $n \geq 1$ and $h \in [1, n]$, there are $2 \cdot \mathit{Tower}(n, h)$ distinct (n, h)-blocks.

▶ **Example 21.** Let $n = 2$ and $h = 2$. In this case $\mathit{Tower}(n, h) = 16$ and $\mathit{Tower}(n, h - 1) = 4$. We can encode by $(2, 2)$-blocks all the integers in $[0, 15]$. Let us consider the number 14 whose binary code (using $\mathit{Tower}(n, h - 1) = 4$ bits) is given by 0111 (the first bit is the least significant). The $(2, 2)$-block with content 0 encoding number 14 is given by $(\$_2, 0) \cdot bl_0 \cdot \$_2 \cdot bl_1 \cdot \$_2 \cdot bl_2 \cdot \$_2 \cdot bl_3 \cdot (\$_2, 0)$, where bl_i is the $(2, 1)$-block encoding the value and the position of the i^{th} bit in 0111. For example, $bl_2 = (\$_1, 1)(1, 0)(2, 1)(\$_1, 1)$ while $bl_3 = (\$_1, 1)(1, 1)(2, 1)(\$_1, 1)$.

We now show that the $(h - 1)$-level D-descriptors (resp., $(2h - 2)$-level BE-descriptors) associated with distinct (n, h)-blocks are distinct as well.

▶ **Lemma 22.** *Let $n \geq 1$. Then, for each $h \in [1, n]$, distinct (n, h)-blocks have distinct $(h - 1)$-level D-descriptors and distinct $(2h - 2)$-level BE-descriptors.*

Proof. For the fixed $n \geq 1$, the proof of Lemma 22 is by induction on $h \in [1, n]$. For the base case, let $h = 1$. Let bl be an $(n, 1)$-block. By construction bl is a word of length $n + 2$ of the form $bl = (\$_1, bit)(1, bit_1) \dots (n, bit_n)(\$_1, bit)$ where $bit, bit_1, \dots, bit_n \in \{0, 1\}$. Hence, the 0-level D-descriptor $D_0(bl)$ (resp., 0-level BE-descriptor $BE_0(bl)$) of bl is the triple $((\$_1, bit), \{(1, bit_1), \dots, (n, bit_n)\}, (\$_1, bit))$, and the result for $h = 1$ easily follows.

Now, for the induction step, assume that $h \in [2, n]$. Let bl and bl' be two (n, h)-blocks such that $bl \neq bl'$. We need to show that the $(h - 1)$-level D-descriptors (resp., $(2h - 2)$-level BE-descriptors) of bl and bl' are distinct. First, assume that bl and bl' have distinct content: let $(\$_h, bit)$ (resp., $(\$_h, bit')$) be the content of bl (resp., bl'). By hypothesis, $bit \neq bit'$. By construction, it follows that $D_0(bl) \neq D_0(bl')$ and $BE_0(bl) \neq BE_0(bl')$. Hence, $D_{h-1}(bl) \neq D_{h-1}(bl')$ and $BE_{2h-2}(bl) \neq BE_{2h-2}(bl')$ and the result follows.

Now, assume that bl and bl' have the same content. Since bl and bl' are distinct (n, h)-blocks, by construction there is $i \in [0, \mathit{Tower}(n, h - 1) - 1]$ such that the $(n, h - 1)$ sub-block sb_i of bl with index i and the $(n, h - 1)$ sub-block sb'_i of bl' with index i have distinct content.

We first consider the D-descriptors. Let $(D_0(bl), T)$ (resp., $(D_0(bl), T')$) be the $(h-1)$-level D-descriptor of bl (resp., bl'). We show that for each non-empty internal subword w of bl, the $(h-2)$-level D-descriptor $D_{h-2}(w)$ of w is distinct from the $(h-2)$-level descriptor $D_{h-2}(sb'_i)$ of sb'_i. Hence, $D_{h-2}(sb'_i) \notin T$. Since $D_{h-2}(sb'_i) \in T'$, we obtain that $T \neq T'$ and the result follows. Fix a non-empty internal subword w of bl. By hypothesis and construction, there is no subword of bl which coincides with sb'_i. We distinguish the following cases:

- w is an $(n, h-1)$-block. Since w is internal subword of bl and no subword of bl coincides with sb'_i, it hold that $w \neq sb'_i$. Hence, by the induction hypothesis, $D_{h-2}(w) \neq D_{h-2}(sb'_i)$.
- w is a proper subword of some $(n, h-1)$-block. By construction $D_0(w)$ is of the form (p, P, p') such that either $p \notin \{(\$_{h-1}, 0), (\$_{h-1}, 1)\}$ or $p' \notin \{(\$_{h-1}, 0), (\$_{h-1}, 1)\}$. Since the 0-level descriptor of an $(n, h-1)$-block is of the form $((\$_{h-1}, bit), P', (\$_{h-1}, bit))$ for some $bit \in \{0, 1\}$, we obtain that $D_0(w) \neq D_0(sb'_i)$. Hence, $D_{h-2}(w) \neq D_{h-2}(sb'_i)$.
- There is some $(n, h-1)$ sub-block w' of bl such that w' is a proper subword of w. By construction, w contains some occurrence of a symbol in $\{\$_h, (\$_h, 0), (\$_h, 1)\}$. Since such symbols do not occur in an $(n, h-1)$-block, the result holds in this case as well.

It remains to consider the BE-descriptors. Let $(BE_0(bl), T_P, T_S)$ (resp., $(BE_0(bl'), T'_P, T'_S)$) be the $(2h-2)$-level BE-descriptor of bl (resp., bl'), and $w_{sb'_i}$ be the unique proper prefix of bl' having sb'_i as a proper suffix. We show that for each non-empty proper prefix w_p of bl, $BE_{2h-3}(w_{sb'_i}) \neq BE_{2h-3}(w_p)$. Hence, $BE_{2h-3}(w_{sb'_i}) \notin T_P$. Since $BE_{2h-3}(w_{sb'_i}) \in T'_P$, we obtain that $T_P \neq T'_P$ and the result follows. Fix a non-empty proper prefix w_p of bl. Note that since $h \geq 2$, $BE_{2h-3}(w_p)$ is of the form $(BE_0(w_p), R_P, R_S)$ and $BE_{2h-3}(w_{sb'_i})$ is of the form $(BE_0(w_{sb'_i}), R'_P, R'_S)$. Thus, it suffices to prove that $R_S \neq R'_S$. Since a proper suffix of a proper prefix of a word u is an internal word of u and $BE_{2h-4}(sb'_i) \in R'_S$, we just need to show that for each non-empty internal subword u of bl, $BE_{2h-4}(sb'_i) \neq BE_{2h-4}(u)$. For this we proceed as for the case of the D-descriptors but this time we apply the induction hypothesis on the BE_{2h-4}-descriptors. This concludes the proof of Lemma 22. ◀

Proof of Theorem 19. Let $n \geq 1$, a_n be a designated letter in the alphabet Σ_n and $\mathcal{K}_n$ the finite Kripke structure over Σ_n given by $\mathcal{K}_n = (\Sigma_n, \Sigma_n, E_n, Lab_n, a_n)$, where $(a, a') \in E_n$ and $Lab_n(a) = \{a\}$ for all $a, a' \in \Sigma_n$. Hence, the paths of $\mathcal{K}_n$ correspond to the non-empty finite words over Σ_n. We show that for all $k \in [0, n-1]$ and basis $\mathcal{B}$ with $\mathcal{B} \in \{\{B, D\}, \{E, D\}\}$ (resp., $\mathcal{B} = \{B, E\}$), there are $\Omega(Tower(n, k+1))$ distinct k-level (resp., $2k$-level) $\mathcal{B}$-certificates of $\mathcal{K}_n$. Hence, Theorem 19 directly follows. By Remark 20, there are $2 \cdot Tower(n, k+1)$ distinct $(n, k+1)$-blocks. Thus, for the basis $\{B, E\}$, the result directly follows from Lemma 22. For the bases $\{B, D\}$ and $\{E, D\}$, the result follows from Lemma 22 and the fact that words having distinct $2k$-level D-descriptors have distinct $2k$-level BD-descriptors (resp., distinct $2k$-level ED-descriptors) as well. ◀

5 Conclusions

We have addressed open complexity issues about the known approach to model-checking the logic HS, based on abstract representations of paths in Kripke structures (BE-descriptors). In particular, we have proposed a unifying framework for model-checking full HS and large HS-fragments obtained by (i) introducing for each basis $\mathcal{B}$, a specialized type of descriptor ($\mathcal{B}$-descriptor) and (ii) designing an alternating-time MC algorithm with a polynomially bounded number of alternations which is parametric w.r.t. the chosen basis $\mathcal{B}$ and runs in time bounded by the length of $\mathcal{B}$-descriptor certificates. As a main result, for each basis $\mathcal{B}$,

we have provided tight bounds on the length of $\mathcal{B}$-certificates: exponential for the bases $\{B\}$ and $\{E\}$ (which lead to $\mathbf{AEXP_{pol}}$ procedures for the related fragments), and non-elementary for the other bases. Future work will be devoted to solve the hard open question about the existence of an elementary procedure for the MC problem for the full logic, and to settle the exact complexity for model-checking the HS-fragments for the bases $\{B\}$ and $\{E\}$.

References

1 J. F. Allen. Maintaining Knowledge about Temporal Intervals. *Communications of the ACM*, 26(11):832–843, 1983.

2 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 *Proc. 8th IJCAR*, LNAI 9706, pages 389–405. Springer, 2016.

3 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 *Proc. 44th ICALP*, volume 80 of *LIPIcs*, pages 120:1–120:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

4 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. *Inf. Comput.*, 262(Part):241–264, 2018.

5 L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Interval vs. Point Temporal Logic Model Checking: An Expressiveness Comparison. *ACM Trans. Comput. Logic*, 20(1):4:1–4:31, 2019.

6 D. Bresolin, D. Della Monica, V. Goranko, A. Montanari, and G. Sciavicco. The dark side of interval temporal logic: marking the undecidability border. *Annals of Mathematics and Artificial Intelligence*, 71(1-3):41–83, 2014.

7 D. Bresolin, V. Goranko, A. Montanari, and P. Sala. Tableau-based decision procedures for the logics of subinterval structures over dense orderings. *Journal of Logic and Computation*, 20(1):133–166, 2010.

8 D. Bresolin, V. Goranko, A. Montanari, and G. Sciavicco. Propositional interval neighborhood logics: Expressiveness, decidability, and undecidable extensions. *Annals of Pure and Applied Logic*, 161(3):289–304, 2009.

9 E. A. Emerson and J. Y. Halpern. "Sometimes" and "not never" revisited: on branching versus linear time temporal logic. *Journal of the ACM*, 33(1):151–178, 1986.

10 J. Ferrante and C. Rackoff. A Decision Procedure for the First Order Theory of Real Addition with Order. *SIAM Journal of Computation*, 4(1):69–76, 1975.

11 J. Y. Halpern and Y. Shoham. A Propositional Modal Logic of Time Intervals. *Journal of the ACM*, 38(4):935–962, 1991.

12 K. Lodaya. Sharpening the Undecidability of Interval Temporal Logic. In *Proc. 6th ASIAN*, LNCS 1961, pages 290–298. Springer, 2000.

13 A. Lomuscio and J. Michaliszyn. An Epistemic Halpern-Shoham Logic. In *Proc. 23rd IJCAI*, pages 1010–1016, 2013.

14 A. Lomuscio and J. Michaliszyn. Decidability of model checking multi-agent systems against a class of EHS specifications. In *Proc. 21st ECAI*, pages 543–548, 2014.

15 J. Marcinkowski and J. Michaliszyn. The Undecidability of the Logic of Subintervals. *Fundamenta Informaticae*, 131(2):217–240, 2014.

16 A. Molinari, A. Montanari, A. Murano, G. Perelli, and A. Peron. Checking interval properties of computations. *Acta Informatica*, 53(6-8):587–619, 2016.

17 A. Molinari, A. Montanari, and A. Peron. A Model Checking Procedure for Interval Temporal Logics based on Track Representatives. In *Proc. 24th CSL*, pages 193–210, 2015.

18 A. Molinari, A. Montanari, and A. Peron. Complexity of ITL model checking: some well-behaved fragments of the interval logic HS. In *Proc. 22nd TIME*, pages 90–100, 2015.

19 Alberto Molinari, Angelo Montanari, and Adriano Peron. Model checking for fragments of Halpern and Shoham's interval temporal logic based on track representatives. *Inf. Comput.*, 259(3):412–443, 2018.

20 A. Montanari, G. Puppis, and P. Sala. A decidable weakening of Compass Logic based on cone-shaped cardinal directions. *Logical Methods in Computer Science*, 11(4), 2015.

21 B. Moszkowski. *Reasoning About Digital Circuits*. PhD thesis, Dept. of Computer Science, Stanford University, Stanford, CA, 1983.

22 A. Pnueli. The temporal logic of programs. In *Proc. 18th FOCS*, pages 46–57. IEEE, 1977.

23 I. Pratt-Hartmann. Temporal propositions and their logic. *Artificial Intelligence*, 166(1-2):1–36, 2005.

24 P. Roeper. Intervals and Tenses. *Journal of Philosophical Logic*, 9:451–469, 1980.

25 Y. Venema. Expressiveness and Completeness of an Interval Tense Logic. *Notre Dame Journal of Formal Logic*, 31(4):529–547, 1990.