An in-depth investigation of interval temporal logic model checking with regular expressions

An in-Depth Investigation of Interval Temporal Logic Model Checking with Regular Expressions

Laura Bozzelli[1], Alberto Molinari[2], Angelo Montanari[2], and Adriano Peron[1]

[1] University of Napoli "Federico II", Napoli, Italy
[2] University of Udine, Udine, Italy

Abstract. In the last years, the model checking (MC) problem for interval temporal logic (ITL) has received an increasing attention as a viable alternative to the traditional (point-based) temporal logic MC, which can be recovered as a special case. Most results have been obtained by imposing suitable restrictions on interval labeling. In this paper, we overcome such limitations by using regular expressions to define the behavior of proposition letters over intervals in terms of the component states. We first prove that MC for Halpern and Shoham's ITL (HS), extended with regular expressions, is decidable. Then, we show that formulas of a large class of HS fragments, namely, all fragments featuring (a subset of) HS modalities for Allen's relations meets, met-by, starts, and started-by, can be model checked in polynomial working space (MC for all these fragments turns out to be PSPACE-complete).

1 Introduction

Model checking (MC) is commonly recognized as one of the most effective techniques in automatic system verification [2]. It has also been successfully used in databases, e.g., active databases, database-backed web applications, and NoSQL databases, and artificial intelligence, e.g., planning, configuration systems, and multi-agent systems. MC allows one to automatically check whether a model of a given system satisfies a desired property to ensure that it meets the expected behaviour. A good balancing of expressiveness and complexity in the choice of the computational model and the specification formalism is a key factor for the actual exploitation of MC. Systems are usually modeled as finite-state transition graphs (Kripke structures), while properties are commonly expressed by formulas of point-based temporal logics, such as LTL, CTL, and CTL*. Various improvements to the computational model and/or the specification language have been proposed in the literature. As for the former, we mention MC for pushdown systems (see, e.g., [7]), that feature an infinite state space, while for the latter we remind the extensions of LTL with promptness, that make it possible to bound the delay with which a liveness request is fulfilled (see, e.g., [9]).

In this paper, we focus on MC with interval temporal logic (ITL) as the specification language. ITL allows one to deal with relevant temporal properties, such as actions with duration, accomplishments, and temporal aggregations, which are inherently "interval-based" and cannot be properly expressed by point-based temporal logics. In the last years, ITL MC has received an increasing attention

as a viable alternative to the traditional (point-based) temporal logic MC [18], which can be recovered as a special case [4]. ITLs feature intervals, instead of points, as their primitive temporal entities [8, 19, 21], and they have been fruitfully applied in various areas of computer science, including formal verification, computational linguistics, planning, and multi-agent systems [10, 11, 19]. Among ITLs, the landmark is Halpern and Shoham's modal logic of time intervals HS [8]. It features one modality for each of the 13 ordering relations between pairs of intervals (the so-called Allen's relations [1]), apart from equality. Its satisfiability problem is undecidable over all relevant classes of linear orders [8], and most of its fragments are undecidable as well [6, 13]. Some meaningful exceptions are the logic of temporal neighbourhood $\mathsf{A\overline{A}}$ and the logic of sub-intervals D.

The MC problem for HS and its fragments consists in the verification of the correctness of the behaviour of a given system with respect to some relevant interval properties. To make it effective, we need to collect information about states into computation stretches: we interpret each finite computation path as an interval, and we define its labelling on the basis of the labelling of the states that compose it. Most results have been obtained by imposing suitable restrictions on interval labeling: either a proposition letter can be constrained to hold over an interval iff it holds over each component state (homogeneity assumption [20]), or interval labeling can be defined in terms of interval endpoints.

In [14], Molinari et al. deal with MC for full HS over finite Kripke structures, under the homogeneity assumption, according to a state-based semantics that allows branching in the past and in the future. They introduce the fundamental elements of the problem and prove its non-elementary decidability and **PSPACE**-hardness. Since then, the attention was also brought to the fragments of HS, which, similarly to what happens with satisfiability, are often computationally much better [15, 16, 3, 5, 14, 17].

The MC problem for some HS fragments, extended with epistemic operators, has been investigated by Lomuscio and Michaliszyn in [10, 11]. Their semantic assumptions differ from those of [14], making it difficult to compare the two approaches. Formulas are interpreted over the unwinding of the Kripke structure (computation-tree-based semantics [4]), and interval labeling takes into account only the endpoints of intervals. The decidability status of MC for full epistemic HS is still unknown. In [12], Lomuscio and Michaliszyn propose to use regular expressions to define the labeling of proposition letters over intervals in terms of the component states. They prove the decidability of MC with regular expressions for some restricted fragments of epistemic HS, giving rough upper bounds to its computational complexity.

In this paper, we prove that MC for full HS with regular expressions is decidable (Section 4) and that its complexity, when restricted to system models—that is, if we assume the formula to be constant length—is **P**. Then, by exploiting a small-model theorem (Section 5), in Section 6, we show that formulas of a large class of HS fragments, i.e., those featuring (any subset of) HS modalities for the Allen's relations *meets, met-by, started-by*, and *starts* ($\mathsf{A\overline{A}B\overline{B}}$), can be checked in polynomial working space (MC for all these is **PSPACE**-complete).

Due to lack of space, all proofs, as well as some complements, can be found in Appendix A.

2 Preliminaries

We first introduce notation and background knowledge, and then the logic HS.

Let $\mathbb{N}$ be the set of natural numbers. For all $i, j \in \mathbb{N}$, we denote by $[i, j]$, with $i \leq j$, the set of naturals h such that $i \leq h \leq j$. Let Σ be an alphabet, w be a non-empty finite word over Σ, and ε be the empty word. We denote by $|w|$ the length of w. For all $1 \leq i \leq j \leq |w|$, $w(i)$ denotes the i-th letter of w (i is called a w-position), while $w(i, j)$ denotes the finite subword of w given by $w(i) \cdots w(j)$. Let $|w| = n$. We define $\mathrm{fst}(w) = w(1)$ and $\mathrm{lst}(w) = w(n)$. $\mathrm{Pref}(w) = \{w(1, i) \mid 1 \leq i \leq n-1\}$ and $\mathrm{Suff}(w) = \{w(i, n) \mid 2 \leq i \leq n\}$ are the sets of all proper prefixes and suffixes of w, respectively. For $i \in [1, n]$, w^i is a shorthand for $w(1, i)$. The concatenation of two words w and w' is denoted as usual by $w \cdot w'$. Moreover, if $\mathrm{lst}(w) = \mathrm{fst}(w')$, $w \star w'$ represents $w(1, n-1) \cdot w'$.

For all $h, n \geq 0$, let $\mathsf{Tower}(h, n)$ denote a tower of exponentials of height h and argument n: $\mathsf{Tower}(0, n) = n$ and $\mathsf{Tower}(h+1, n) = 2^{\mathsf{Tower}(h,n)}$. Moreover, let h-**EXPTIME** denote the class of languages decided by deterministic Turing machines whose number of computation steps is bounded by functions of n in $O(\mathsf{Tower}(h, n^c))$, for some constant $c \geq 1$. Note that 0-**EXPTIME** is **P**.

2.1 Kripke structures, regular expressions, and finite automata

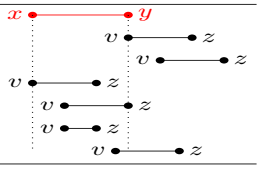
Finite state systems are usually modelled as finite Kripke structures. Let $\mathcal{AP}$ be a finite set of proposition letters, which represent predicates over the states of the given system.

Definition 1 (Kripke structure). *A* Kripke structure *is a tuple* $\mathcal{K} = (\mathcal{AP}, S, R, \mu, s_0)$*, where* S *is a set of states,* $R \subseteq S \times S$ *is a left-total transition relation,* $\mu : S \mapsto 2^{\mathcal{AP}}$ *is a total labelling function assigning to each state* s *the set of proposition letters that hold over it, and* $s_0 \in S$ *is the initial state. For* $s \in S$*, the set* $R(s)$ *of successors of* s *is the non-empty set of states* s' *such that* $(s, s') \in R$*. We say that* $\mathcal{K}$ *is finite if* S *is finite.*

Let $\mathcal{K} = (\mathcal{AP}, S, R, \mu, s_0)$ be a Kripke structure. A *trace* of $\mathcal{K}$ is a non-empty finite word ρ over S such that $(\rho(i), \rho(i+1)) \in R$ for $i \in [1, |\rho| - 1]$. A trace is *initial* if it starts from s_0. We denote by $\mathrm{Trc}_{\mathcal{K}}$ the *infinite* set of traces of $\mathcal{K}$. A trace ρ induces the finite word $\mu(\rho)$ over $2^{\mathcal{AP}}$ given by $\mu(\rho(1)) \dots \mu(\rho(n))$, with $n = |\rho|$. We call $\mu(\rho)$ the *labeling sequence* induced by ρ.

Let us now introduce the class of regular expressions over finite words. Since we are interested in expressing requirements over the labeling sequences induced by the traces of Kripke structures, here we consider *proposition-based* regular expressions (RE), where atomic expressions are propositional formulas over $\mathcal{AP}$ instead of letters over an alphabet. Formally, the set of RE r over $\mathcal{AP}$ is defined as $r ::= \varepsilon \mid \phi \mid r \cup r \mid r \cdot r \mid r^*$ where ϕ is a propositional formula over $\mathcal{AP}$. The length $|r|$ of an RE r is the number of subexpressions of r. An RE r denotes a language $\mathcal{L}(r)$ of finite words over $2^{\mathcal{AP}}$ defined as: (*i*) $\mathcal{L}(\varepsilon) = \{\varepsilon\}$ and $\mathcal{L}(\phi) = \{A \in 2^{\mathcal{AP}} \mid A \text{ satisfies } \phi\}$; (*ii*) $\mathcal{L}(r_1 \cup r_2) = \mathcal{L}(r_1) \cup \mathcal{L}(r_2)$, $\mathcal{L}(r_1 \cdot r_2) = \mathcal{L}(r_1) \cdot \mathcal{L}(r_2)$, and $\mathcal{L}(r^*) = (\mathcal{L}(r))^*$. By well-known results, the class of RE over $\mathcal{AP}$ captures the class of regular languages of finite words over $2^{\mathcal{AP}}$.

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

A non-deterministic finite automaton (NFA) is a tuple $\mathcal{A} = (\Sigma, Q, Q_0, \delta, F)$, where Σ is a finite alphabet, Q is a finite set of states, $Q_0 \subseteq Q$ is the set of initial states, $\delta : Q \times \Sigma \mapsto 2^Q$ is the transition function, and $F \subseteq Q$ is the set of accepting states. Given a finite word w over Σ, with $|w| = n$, and two states $q, q' \in Q$, a run (or computation) of $\mathcal{A}$ from q to q' over w is a finite sequence of states $q_1, \ldots, q_{n+1}$ such that $q_1 = q$, $q_{n+1} = q'$, and for all $i \in [1, n]$, $q_{i+1} \in \delta(q_i, w(i))$. The language $\mathcal{L}(\mathcal{A})$ accepted by $\mathcal{A}$ consists of the finite words w over Σ such that there is a run from some initial state to some accepting state over w. A deterministic finite automaton (DFA) is an NFA $\mathcal{D} = (\Sigma, Q, Q_0, \delta, F)$ such that Q_0 is a singleton and for all $(q, c) \in Q \times \Sigma$, $\delta(q, c)$ is a singleton.

Remark 2. By well-known results, given an RE r over $\mathcal{AP}$, one can construct, in a compositional way, an NFA $\mathcal{A}_r$ over $2^{\mathcal{AP}}$, whose number of states is at most $2|r|$, such that $\mathcal{L}(\mathcal{A}_r) = \mathcal{L}(r)$. We call $\mathcal{A}_r$ the *canonical* NFA associated with r. Note that the number of edges of $\mathcal{A}_r$ may be exponential in $|\mathcal{AP}|$ (edges are labelled by assignments $A \in 2^{\mathcal{AP}}$ satisfying propositional formulas ϕ of r); however, we can avoid storing edges, as they can be recovered in polynomial time from r.

2.2 The interval temporal logic HS

An interval algebra to reason about intervals and their relative order 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 [8]. 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 (the inverse $\overline{\mathcal{R}}$ of a binary relation $\mathcal{R}$ is such that $b\overline{\mathcal{R}}a$ iff $a\mathcal{R}b$) and equality. Moreover, if $\langle X \rangle$ is the modality for $\mathcal{R}$, $\langle \overline{X} \rangle$ is the modality for $\overline{\mathcal{R}}$.

Let $\mathcal{P}_u$ be a finite set of *uninterpreted interval properties*. The HS language over $\mathcal{P}_u$ consists of proposition letters from $\mathcal{P}_u$, the Boolean connectives $\neg$ and $\wedge$, and a temporal modality for each of the (non trivial) Allen's relations, i.e., $\langle \mathrm{A} \rangle$, $\langle \mathrm{L} \rangle$, $\langle \mathrm{B} \rangle$, $\langle \mathrm{E} \rangle$, $\langle \mathrm{D} \rangle$, $\langle \mathrm{O} \rangle$, $\langle \overline{\mathrm{A}} \rangle$, $\langle \overline{\mathrm{L}} \rangle$, $\langle \overline{\mathrm{B}} \rangle$, $\langle \overline{\mathrm{E}} \rangle$, $\langle \overline{\mathrm{D}} \rangle$, and $\langle \overline{\mathrm{O}} \rangle$. HS formulas are defined by the grammar $\psi ::= p_u \mid \neg\psi \mid \psi \wedge \psi \mid \langle X \rangle \psi \mid \langle \overline{X} \rangle \psi$, where $p_u \in \mathcal{P}_u$ and $X \in \{A, L, B, E, D, O\}$. We will also use the standard connectives (disjunction $\vee$ and implication $\rightarrow$). Moreover, for any modality X, the dual universal modalities $[X]\psi$ and $[\overline{X}]\psi$ are defined as $\neg\langle X \rangle \neg\psi$ and $\neg\langle \overline{X} \rangle \neg\psi$, respectively. Given any subset of Allen's relations $\{X_1, \ldots, X_n\}$, we denote by $\mathsf{X_1} \cdots \mathsf{X_n}$ the HS fragment that features existential (and universal) modalities for $X_1, \ldots, X_n$ only. W.l.o.g., we assume the *non-strict semantics of HS*, which admits intervals consisting of

a single point[3]. Under such an assumption, all HS modalities can be expressed in terms of modalities $\langle \mathrm{B} \rangle, \langle \mathrm{E} \rangle, \langle \overline{\mathrm{B}} \rangle$, and $\langle \overline{\mathrm{E}} \rangle$ [21]. HS can thus be viewed as a multi-modal logic with 4 primitive modalities. However, since later we will focus on the HS fragments $\mathsf{A\overline{A}E\overline{E}}$ and $\mathsf{A\overline{A}B\overline{B}}$—which respectively do not feature $\langle \mathrm{B} \rangle$, $\langle \overline{\mathrm{B}} \rangle$ and $\langle \mathrm{E} \rangle$, $\langle \overline{\mathrm{E}} \rangle$—we add both $\langle \mathrm{A} \rangle$ and $\langle \overline{\mathrm{A}} \rangle$ to the considered set of modalities.

In [14], the authors investigate the MC problem over finite Kripke structures $\mathcal{K}$ for HS formulas where intervals correspond to the traces of $\mathcal{K}$. The approach followed there is subject to two restrictions: (*i*) the set $\mathcal{P}_u$ of HS-proposition letters and the set $\mathcal{AP}$ of proposition letters for the Kripke structure coincide, and (*ii*) a proposition letter holds over an interval iff it holds over all its sub-intervals (homogeneity assumption). Here, we adopt a more general and expressive approach according to which an abstract interval proposition letter $p_u \in \mathcal{P}_u$ denotes a regular language of finite words over $2^{\mathcal{AP}}$, that is, every p_u is a (proposition-based) regular expression over $\mathcal{AP}$. Thus, hereafter, an HS formula over $\mathcal{AP}$ is an HS formula whose interval proposition letters (or atomic formulas) are RE r over $\mathcal{AP}$. Given a Kripke structure $\mathcal{K} = (\mathcal{AP}, S, R, \mu, s_0)$, a trace ρ of $\mathcal{K}$, and an HS formula φ over $\mathcal{AP}$, the satisfaction relation $\mathcal{K}, \rho \models \varphi$ is inductively defined as follows (we omit the standard clauses for Boolean connectives):

- $\mathcal{K}, \rho \models r$ iff $\mu(\rho) \in \mathcal{L}(r)$ for each RE r over $\mathcal{AP}$,
- $\mathcal{K}, \rho \models \langle \mathrm{B} \rangle \varphi$ iff there exists $\rho' \in \mathrm{Pref}(\rho)$ such that $\mathcal{K}, \rho' \models \varphi$,
- $\mathcal{K}, \rho \models \langle \mathrm{E} \rangle \varphi$ iff there exists $\rho' \in \mathrm{Suff}(\rho)$ such that $\mathcal{K}, \rho' \models \varphi$,
- $\mathcal{K}, \rho \models \langle \overline{\mathrm{B}} \rangle \varphi$ iff $\mathcal{K}, \rho' \models \varphi$ for some trace ρ' such that $\rho \in \mathrm{Pref}(\rho')$,
- $\mathcal{K}, \rho \models \langle \overline{\mathrm{E}} \rangle \varphi$ iff $\mathcal{K}, \rho' \models \varphi$ for some trace ρ' such that $\rho \in \mathrm{Suff}(\rho')$.

$\mathcal{K}$ is a *model* of φ, denoted as $\mathcal{K} \models \varphi$, if for all *initial* traces ρ of $\mathcal{K}$, it holds that $\mathcal{K}, \rho \models \varphi$. The *MC problem* for HS is the problem of checking, for a finite Kripke structure $\mathcal{K}$ and an HS formula φ, whether or not $\mathcal{K} \models \varphi$. The problem is not trivially decidable since the set $\mathrm{Trc}_{\mathcal{K}}$ of traces of $\mathcal{K}$ is infinite.

3 The general picture

Here we give a short account of research on MC for HS and its fragments, and we enlighten the original contributions of the present paper (see Table 2).

Let us consider first the MC problem for HS and its fragments, under the homogeneity assumption, according to a state-based semantics [4]. In [14], Molinari et al. provide a MC algorithm for (full) HS, with a non-elementary complexity, that, given a finite Kripke structure $\mathcal{K}$ and a bound k on the nesting depth of $\langle \mathrm{E} \rangle$ and $\langle \mathrm{B} \rangle$ modalities in the input HS formula, exploits a *finite* and satisfiability-equivalent representation for the infinite set $\mathrm{Trc}_{\mathcal{K}}$, that accounts for $\mathcal{K}$ and k. **EXPSPACE**-hardness of BE, and thus of full HS, has been shown in [3]. An **EXPSPACE** MC algorithm for the fragments $\mathsf{A\overline{A}B\overline{B}E\overline{E}}$ and $\mathsf{A\overline{A}E\overline{B}E\overline{E}}$ has been devised in [16]. A number of well-behaved HS fragments, whose MC problem has a computational complexity markedly lower than that of full HS, have been identified in [3, 5, 15, 17], where MC has been proved to be (*i*) **PSPACE**-complete for $\mathsf{A\overline{A}BE\overline{E}}$, $\mathsf{A\overline{A}B\overline{B}}$, $\mathsf{A\overline{A}E\overline{E}}$, $\overline{\mathsf{B}}$, and $\overline{\mathsf{E}}$, (*ii*) $\mathbf{P}^{\mathbf{NP}}$-complete for AB, $\mathsf{A\overline{A}B}$, $\mathsf{\overline{A}E}$, and

[3] All the results we prove in the paper hold for the strict semantics as well.

Table 2. Complexity of MC for HS and its fragments (†local MC).

	Homogeneity	Regular expressions	Endpoints + KC
Full HS, BE	non-elem. **EXPSPACE**-hard	non-elem. **EXPSPACE**-hard	BE+$KC^\dagger$: **PSPACE** BE†: **P**
$\mathsf{A\overline{A}B\overline{B}E}$, $\mathsf{A\overline{A}E\overline{B}E}$	**EXPSPACE** **PSPACE**-hard	non-elem. **PSPACE**-hard	
$\mathsf{A\overline{A}B\overline{E}}$	**PSPACE**-c.	non-elem. **PSPACE**-hard	
$\mathsf{A\overline{A}B\overline{B}}$, $\mathsf{B\overline{B}}$, $\mathsf{\overline{B}}$, $\mathsf{A\overline{A}E\overline{E}}$, $\mathsf{E\overline{E}}$, $\mathsf{\overline{E}}$	**PSPACE**-c.	**PSPACE**-c.	$\mathsf{A\overline{B}}$+KC: non-elem.
$\mathsf{A\overline{A}B}$, $\mathsf{A\overline{A}E}$, AB, $\mathsf{\overline{A}E}$	$\mathbf{P}^{\mathbf{NP}}$-c.	**PSPACE**-c.	
$\mathsf{A\overline{A}}$, $\mathsf{\overline{A}B}$, AE, A, $\mathsf{\overline{A}}$	$\mathbf{P}^{\mathbf{NP}[O(\log^2 n)]}$ $\mathbf{P}^{\mathbf{NP}[O(\log n)]}$-hard	**PSPACE**-c.	
Prop, B, E	**co-NP**-c.	**PSPACE**-c.	

$\mathsf{A\overline{A}E}$, (*iii*) in between $\mathbf{P}^{\mathbf{NP}[O(\log n)]}$ and $\mathbf{P}^{\mathbf{NP}[O(\log^2 n)]}$ for $\mathsf{A\overline{A}}$, A, $\mathsf{\overline{A}}$, $\mathsf{\overline{A}B}$, and AE, and (*iv*) **co-NP**-complete for B, E, and Prop (the pure propositional fragment).

In [10, 11], Lomuscio and Michaliszyn investigate MC for some HS fragments extended with the epistemic modalities K and C, according to a computation-tree-based semantics [4], under the assumption that interval labeling is defined by interval endpoints only. They prove that *local* MC for BE+KC is **PSPACE**-complete (it is in **P** for BE), and they give a non-elementary upper bound to the complexity of MC for $\mathsf{A\overline{B}}$+KC. Later, in [12], they propose an alternative definition of interval labeling for the two fragments, which associates a regular expression over the set of states of the Kripke structure with each proposition letter, that leads to a significant increase in expressiveness, at no extra computational cost. Nothing is said about MC for full HS (with or without K, C).

In this paper, we define interval labeling via regular expressions in a way that can be shown to be equivalent to that of [12]. We first show that MC for (full) HS with regular expressions and state-based semantics is decidable. Then, we prove that relaxing the homogeneity assumption via regular expressions comes at no cost for $\mathsf{A\overline{A}B\overline{B}}$, $\mathsf{A\overline{A}E\overline{E}}$, $\mathsf{B\overline{B}}$, $\mathsf{E\overline{E}}$, $\mathsf{\overline{B}}$, and $\mathsf{\overline{E}}$, that remain in **PSPACE**, while $\mathsf{A\overline{A}B}$ and $\mathsf{A\overline{A}E}$ and their fragments increase their complexity to **PSPACE**. Since the computation-tree-based semantics and the state-based one behave exactly in the same way when restricted to HS fragments featuring present and future modalities only[4], from the **PSPACE**-completeness of $\mathsf{A\overline{A}B\overline{B}}$, it immediately follows the **PSPACE** membership of $\mathsf{A\overline{B}}$ with regular expressions, devoid of epistemic operators (in fact, the non-elementary complexity of MC for $\mathsf{A\overline{B}}$ in [12] can be hardly ascribed to the addition of epistemic operators). The definitions of interval labeling given in [14] and [10, 11] can be recovered as special cases of the present one as follows. To force homogeneity, all regular expressions in the formula have to be of the form $p \cdot p^*$, for $p \in \mathcal{AP}$, while interval labeling based on endpoints is captured by regular expressions of the form $\bigcup_{(i,j)\in I}(q_i \cdot \top^* \cdot q_j) \cup \bigcup_{i\in I'} q_i$, for some suitable $I \subseteq \{1, \ldots, |S|\}^2$, $I' \subseteq \{1, \ldots, |S|\}$, where $q_i \in \mathcal{AP}$ is a letter labeling the state $s_i \in S$ of $\mathcal{K}$ only.

[4] As shown in [4], this is not the case in general: the computation-tree-based semantics of [10–12] is subsumed by the state-based one of [14] and follow-up papers.

4 MC for full HS

In this section, we give an automata-theoretic solution to the MC problem for full HS. Given a finite Kripke structure $\mathcal{K}$ and an HS formula φ over $\mathcal{AP}$, we compositionally construct an NFA over the set of states of $\mathcal{K}$ accepting the set of traces ρ of $\mathcal{K}$ such that $\mathcal{K}, \rho \models \varphi$. The size of the resulting NFA is nonelementary, but it is just *linear in the size of* $\mathcal{K}$. To ensure that the non-elementary blow-up does not depend on the size of $\mathcal{K}$, we introduce a special subclass of NFAs, that we call $\mathcal{K}$-NFA. Let $\mathcal{K} = (\mathcal{AP}, S, R, \mu, s_0)$ be a Kripke structure over $\mathcal{AP}$.

Definition 3. *A $\mathcal{K}$-NFA is an NFA $\mathcal{A} = (S, Q, Q_0, \delta, F)$ over S satisfying: (i) the set Q of states is of the form $M \times S$ (M is called the* main component *or the set of* main states*); (ii) $Q_0 \cap F = \emptyset$, i.e., the empty word ε is not accepted; (iii) for all $(q, s) \in M \times S$ and $s' \in S$, $\delta((q, s), s') = \emptyset$ if $s' \neq s$, and $\delta((q, s), s) \subseteq M \times R(s)$.*

Note that a $\mathcal{K}$-NFA $\mathcal{A}$ accepts only traces of $\mathcal{K}$. Moreover, for all words $\rho \in S^+$, if there is a run of $\mathcal{A}$ over ρ, then ρ is a trace of $\mathcal{K}$.

Proposition 4. *Let $\mathcal{A}$ be an NFA over $2^{\mathcal{AP}}$ with n states. One can construct in polynomial time a $\mathcal{K}$-NFA $\mathcal{A}_{\mathcal{K}}$ with at most $n + 1$ main states accepting the set of traces ρ of $\mathcal{K}$ such that $\mu(\rho) \in \mathcal{L}(\mathcal{A})$.*

Proof. Let $\mathcal{A} = (2^{\mathcal{AP}}, Q, Q_0, \delta, F)$. By using an additional state, we can assume $\varepsilon \notin \mathcal{L}(\mathcal{A})$ (i.e., $Q_0 \cap F = \emptyset$). Then, $\mathcal{A}_{\mathcal{K}} = (S, Q \times S, Q_0 \times S, \delta', F \times S)$, where for all $(q, s) \in Q \times S$ and $s' \in S$, $\delta'((q, s), s') = \emptyset$ if $s' \neq s$, and $\delta'((q, s), s) = \delta(q, \mu(s)) \times R(s)$. Since $R(s) \neq \emptyset$ for all $s \in S$, the thesis follows. □

We now extend the semantics of the HS modalities $\langle \mathrm{B} \rangle$, $\langle \overline{\mathrm{B}} \rangle$, $\langle \mathrm{E} \rangle$, $\langle \overline{\mathrm{E}} \rangle$ over $\mathcal{K}$ to languages $\mathcal{L}$ of finite words over S. Given any such language $\mathcal{L}$ over S, let $\langle \mathrm{B} \rangle_{\mathcal{K}}(\mathcal{L})$, $\langle \mathrm{E} \rangle_{\mathcal{K}}(\mathcal{L})$, $\langle \overline{\mathrm{B}} \rangle_{\mathcal{K}}(\mathcal{L})$, $\langle \overline{\mathrm{E}} \rangle_{\mathcal{K}}(\mathcal{L})$ be the languages of traces of $\mathcal{K}$ defined as:

- $\langle \mathrm{B} \rangle_{\mathcal{K}}(\mathcal{L}) = \{\rho \in \mathrm{Trc}_{\mathcal{K}} \mid \exists\, \rho' \in \mathcal{L} \cap S^+ \text{ and } \rho'' \in S^+ \text{ such that } \rho = \rho' \cdot \rho''\}$,
- $\langle \overline{\mathrm{B}} \rangle_{\mathcal{K}}(\mathcal{L}) = \{\rho \in \mathrm{Trc}_{\mathcal{K}} \mid \exists\, \rho' \in S^+ \text{ such that } \rho \cdot \rho' \in \mathcal{L} \cap \mathrm{Trc}_{\mathcal{K}}\}$,
- $\langle \mathrm{E} \rangle_{\mathcal{K}}(\mathcal{L}) = \{\rho \in \mathrm{Trc}_{\mathcal{K}} \mid \exists\, \rho'' \in \mathcal{L} \cap S^+ \text{ and } \rho' \in S^+ \text{ such that } \rho = \rho' \cdot \rho''\}$,
- $\langle \overline{\mathrm{E}} \rangle_{\mathcal{K}}(\mathcal{L}) = \{\rho \in \mathrm{Trc}_{\mathcal{K}} \mid \exists\, \rho' \in S^+ \text{ such that } \rho' \cdot \rho \in \mathcal{L} \cap \mathrm{Trc}_{\mathcal{K}}\}$.

The compositional translation of HS formulas into a $\mathcal{K}$-NFA is based on the following two propositions. First, we show that $\mathcal{K}$-NFAs are closed under the above language operations.

Proposition 5. *Given a $\mathcal{K}$-NFA $\mathcal{A}$ with n main states, one can construct in polynomial time $\mathcal{K}$-NFAs with $n + 1$ main states accepting the languages $\langle \mathrm{B} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$, $\langle \mathrm{E} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$, $\langle \overline{\mathrm{B}} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$, and $\langle \overline{\mathrm{E}} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$, respectively.*

Proof. Let $\mathcal{A} = (S, M \times S, Q_0, \delta, F)$ be the given $\mathcal{K}$-NFA, where M is the set of main states. We omit the constructions for $\langle \mathrm{E} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$ and $\langle \overline{\mathrm{E}} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$ (which are symmetric to those for $\langle \mathrm{B} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$ and $\langle \overline{\mathrm{B}} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$, respectively).

Construction for the language $\langle \mathrm{B} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$. Let us consider the NFA $\mathcal{A}_{\langle \mathrm{B} \rangle}$ over S given by $\mathcal{A}_{\langle \mathrm{B} \rangle} = (S, (M \cup \{q_{acc}\}) \times S, Q_0, \delta', \{q_{acc}\} \times S)$, where $q_{acc} \notin M$ is a

fresh main state, and for all $(q,s) \in (M \cup \{q_{acc}\}) \times S$ and $s' \in S$, $\delta'((q,s),s') = \emptyset$, if $s' \neq s$, and $\delta'((q,s),s)$ is defined as follows:

$$\delta'((q,s),s) = \begin{cases} \delta((q,s),s) & \text{if } (q,s) \in (M \times S) \setminus F \\ \delta((q,s),s) \cup (\{q_{acc}\} \times R(s)) & \text{if } (q,s) \in F \\ \{q_{acc}\} \times R(s) & \text{if } q = q_{acc}. \end{cases}$$

Given an input word ρ, from an initial state (q_0,s) of $\mathcal{A}$, the automaton $\mathcal{A}_{\langle \mathrm{B} \rangle}$ simulates the behavior of $\mathcal{A}$ from (q_0,s) over ρ, but when $\mathcal{A}$ is in an accepting state (q_f,s) and the current input symbol is s, $\mathcal{A}_{\langle \mathrm{B} \rangle}$ can additionally choose to move to a state in $\{q_{acc}\} \times R(s)$, which is accepting for $\mathcal{A}_{\langle \mathrm{B} \rangle}$. From such states, $\mathcal{A}_{\langle \mathrm{B} \rangle}$ accepts iff the remaining portion of the input is a trace of $\mathcal{K}$. Formally, by construction, since $\mathcal{A}$ is a $\mathcal{K}$-NFA, $\mathcal{A}_{\langle \mathrm{B} \rangle}$ is a $\mathcal{K}$-NFA as well. Moreover, a word ρ over S is accepted by $\mathcal{A}_{\langle \mathrm{B} \rangle}$ *iff* ρ is a trace of $\mathcal{K}$ having some proper prefix ρ' in $\mathcal{L}(\mathcal{A})$ (note that $\rho' \neq \varepsilon$ since $\mathcal{A}$ is a $\mathcal{K}$-NFA). Hence, $\mathcal{L}(\mathcal{A}_{\langle \mathrm{B} \rangle}) = \langle \mathrm{B} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$.

Construction for the language $\langle \overline{\mathrm{B}} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$. Let us consider the NFA $\mathcal{A}_{\langle \overline{\mathrm{B}} \rangle}$ over S given by $\mathcal{A}_{\langle \overline{\mathrm{B}} \rangle} = (S, (M \cup \{q_0'\}) \times S, \{q_0'\} \times S, \delta', F')$, where $q_0' \notin M$ is a fresh main state and δ' and F' are defined as follows: (i) for all $(q,s) \in (M \cup \{q_0'\}) \times S$ and $s' \in S$, $\delta'((q,s),s') = \emptyset$ if $s' \neq s$, and $\delta'((q,s),s)$ is defined as follows:

$$\delta'((q,s),s) = \begin{cases} \bigcup\limits_{(q_0,s) \in Q_0} \delta((q_0,s),s) & \text{if } q = q_0' \\ \delta((q,s),s) & \text{otherwise.} \end{cases}$$

(ii) The set F' of accepting states is the set of states (q,s) of $\mathcal{A}$ such that there is a run of $\mathcal{A}$ from (q,s) to some state in F over some non-empty word. It easily follows by construction that $\mathcal{A}_{\langle \overline{\mathrm{B}} \rangle}$ is a $\mathcal{K}$-NFA and $\mathcal{L}(\mathcal{A}_{\langle \overline{\mathrm{B}} \rangle}) = \langle \overline{\mathrm{B}} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$. □

We now show that $\mathcal{K}$-NFAs are closed under Boolean operations.

Proposition 6. *Given two $\mathcal{K}$-NFAs $\mathcal{A}$ and $\mathcal{A}'$ with n and n' main states, respectively, one can construct:*
- *in time $O(n+n')$ a $\mathcal{K}$-NFA with $n+n'$ main states accepting $\mathcal{L}(\mathcal{A}) \cup \mathcal{L}(\mathcal{A}')$;*
- *in time $2^{O(n)}$ a $\mathcal{K}$-NFA with $2^{n+1}+1$ main states accepting $\mathrm{Trc}_{\mathcal{K}} \setminus \mathcal{L}(\mathcal{A})$.*

Proof. We omit the construction for union, as it is a natural generalization of the one for NFAs, and focus on complementation. Let $\mathcal{A} = (S, M \times S, Q_0, \delta, F)$. Let n be the number of main states of $\mathcal{A}$. First, we need a preliminary construction. Let us consider the NFA $\mathcal{A}'' = (S, (M \cup \{q_{acc}\}) \times S, Q_0, \delta'', \{q_{acc}\} \times S)$, where $q_{acc} \notin M$ is a fresh main state, and for all $(q,s) \in (M \cup \{q_{acc}\}) \times S$ and $s' \in s$, $\delta''((q,s),s') = \emptyset$ if $s' \neq s$, and

$$\delta''((q,s),s) = \begin{cases} \delta((q,s),s) \cup (\{q_{acc}\} \times S) & \text{if } q \in M \text{ and } \delta((q,s),s) \cap F \neq \emptyset \\ \delta((q,s),s) & \text{if } q \in M \text{ and } \delta((q,s),s) \cap F = \emptyset \\ \emptyset & \text{if } q = q_{acc}. \end{cases}$$

Note that $\mathcal{A}''$ is *not* a $\mathcal{K}$-NFA. However, $\mathcal{L}(\mathcal{A}'') = \mathcal{L}(\mathcal{A})$.

Next we show that it is possible to construct in time $2^{O(n)}$ a *weak* $\mathcal{K}$-NFA $\mathcal{A}_c$ with 2^{n+1} main states accepting $(\mathrm{Trc}_{\mathcal{K}} \setminus \mathcal{L}(\mathcal{A}'')) \cup \{\varepsilon\}$, where a *weak* $\mathcal{K}$-NFA is a $\mathcal{K}$-NFA but the requirement that the empty word ε is not accepted is relaxed. Thus, since a weak $\mathcal{K}$-NFA can be easily converted into an equivalent $\mathcal{K}$-NFA by using an additional main state and $\mathcal{L}(\mathcal{A}'') = \mathcal{L}(\mathcal{A})$, the result follows. Let $\tilde{M} = M \cup \{q_{acc}\}$. Then, the weak $\mathcal{K}$-NFA $\mathcal{A}_c$ is given by $\mathcal{A}_c = (S, 2^{\tilde{M}} \times S, Q_{0,c}, \delta_c, F_c)$, where $Q_{0,c}$, F_c, and δ_c are defined as follows: (i) $Q_{0,c} = \{(P, s) \in 2^M \times S \mid P = \{q \in M \mid (q, s) \in Q_0\}\}$; (ii) $F_c = \{(P, s) \in 2^M \times S\}$; (iii) for all $(P, s) \in 2^{\tilde{M}} \times S$ and $s' \in S$, $\delta_c((P, s), s') = \emptyset$ if $s' \neq s$, and $\delta_c((P, s), s)$ is given by

$$\bigcup_{s' \in R(s)} \Big\{ (\{q' \in \tilde{M} \mid (q', s') \in \bigcup_{p \in P} \delta''(p, s)\}, s') \Big\}.$$

By construction, $\mathcal{A}_c$ is a weak $\mathcal{K}$-NFA. Hence $\mathcal{A}_c$ does not accept words in $S^+ \setminus \mathrm{Trc}_{\mathcal{K}}$. Moreover, by construction, $Q_{0,c} \subseteq F$, thus $\varepsilon \in \mathcal{L}(\mathcal{A}_c)$. Finally it is easy to prove that $\rho \in \mathcal{L}(\mathcal{A}'')$ if and only if $\rho \notin \mathcal{L}(\mathcal{A}_c)$. □

Let φ be an HS formula. We can convert φ into an equivalent formula, called *existential form of* φ, that makes use of negations, disjunctions, and the existential modalities $\langle \mathrm{B} \rangle$, $\langle \overline{\mathrm{B}} \rangle$, $\langle \mathrm{E} \rangle$, $\langle \overline{\mathrm{E}} \rangle$, only. For all $h \geq 1$, HS_h denotes the syntactical HS fragment consisting only of formulas φ such that the nesting depth of negation in the existential form of φ is at most h. Moreover $\neg\mathsf{HS}_h$ is the set of formulas φ such that $\neg\varphi \in \mathsf{HS}_h$. Given an HS formula φ, checking whether $\mathcal{K} \not\models \varphi$ reduces to checking the existence of an initial trace ρ of $\mathcal{K}$ such that $\mathcal{K}, \rho \models \neg\varphi$.

The next theorem concludes this section by stating its main result.

Theorem 7. *There exists a constant c such that, given a finite Kripke structure $\mathcal{K}$ and an HS formula φ, one can construct a $\mathcal{K}$-NFA with $O(|\mathcal{K}| \cdot \mathsf{Tower}(h, |\varphi|^c))$ states accepting the set of traces ρ of $\mathcal{K}$ such that $\mathcal{K}, \rho \models \varphi$, where h is the nesting depth of negation in the existential form of φ.*

*Moreover, for each $h \geq 0$, the MC problem for $\neg\mathsf{HS}_h$ is in h-***EXPTIME***. Additionally, for a constant-length formula, the MC problem is in* **P**.

5 Exponential Small-Model for $\mathsf{A\overline{A}B\overline{B}}$ and $\mathsf{A\overline{A}E\overline{E}}$

Here we prove an exponential small-model property for the fragments $\mathsf{A\overline{A}B\overline{B}}$ and $\mathsf{A\overline{A}E\overline{E}}$, that is, if a trace ρ of a finite Kripke structure $\mathcal{K}$ satisfies a formula φ of $\mathsf{A\overline{A}B\overline{B}}$ or $\mathsf{A\overline{A}E\overline{E}}$, then there exists a trace π, whose length is exponential in the sizes of φ and $\mathcal{K}$, starting from and leading to the same states as ρ, that satisfies φ. We focus on $\mathsf{A\overline{A}B\overline{B}}$ (being the case for $\mathsf{A\overline{A}E\overline{E}}$ symmetric). Let $\mathcal{K} = (\mathcal{AP}, S, R, \mu, s_0)$ be a finite Kripke structure. We start by introducing the notion of *trace induced* by a trace ρ which is obtained by contracting ρ, concatenating some subtraces of ρ (provided that the resulting sequence is another trace of $\mathcal{K}$).

Definition 8. *Let $\rho \in \mathrm{Trc}_{\mathcal{K}}$ be a trace with $|\rho| = n$. A* trace induced by ρ *is a trace $\pi \in \mathrm{Trc}_{\mathcal{K}}$ such that there exists an increasing sequence of ρ-positions $i_1 < \ldots < i_k$, with $i_1 = 1$, $i_k = n$, and $\pi = \rho(i_1) \cdots \rho(i_k)$. Moreover, we say that the π-position j and the ρ-position i_j are* corresponding.

Note that if π is induced by ρ, then $\mathrm{fst}(\pi) = \mathrm{fst}(\rho)$, $\mathrm{lst}(\pi) = \mathrm{lst}(\rho)$, and $|\pi| \leq |\rho|$.

Given a DFA $\mathcal{D} = (\Sigma, Q, q_0, \delta, F)$, we denote by $\mathcal{D}(w)$ (resp., $\mathcal{D}_q(w)$) the state reached by the computation of $\mathcal{D}$ from q_0 (resp., $q \in Q$) over the word $w \in \Sigma^*$.

We now consider *well-formedness* of induced traces w.r.t. a set of DFAs: a well formed trace π induced by ρ preserves the states of the computations of the DFAs reached by reading prefixes of ρ and π bounded by corresponding positions.

Definition 9. *Let $\mathcal{K} = (\mathcal{AP}, S, R, \mu, s_0)$ be a finite Kripke structure, $\rho \in \mathrm{Trc}_{\mathcal{K}}$ be a trace, and $\mathcal{D}^s = (2^{\mathcal{AP}}, Q^s, q_0^s, \delta^s, F^s)$ with $s = 1, \ldots, k$, be DFAs. A trace $\pi \in \mathrm{Trc}_{\mathcal{K}}$* induced by *$\rho$ is $(q^1_{\ell_1}, \ldots, q^k_{\ell_k})$*-well-formed w.r.t. *$\rho$, with $q^s_{\ell_s} \in Q^s$ for all $s = 1, \ldots, k$, if and only if for all π-positions j, with corresponding ρ-positions i_j, and all $s = 1, \ldots, k$, it holds that $\mathcal{D}^s_{q^s_{\ell_s}}(\mu(\pi^j)) = \mathcal{D}^s_{q^s_{\ell_s}}(\mu(\rho^{i_j}))$.*

For $q^s_{\ell_s} \in Q^s$, $s = 1, \ldots, k$, the $(q^1_{\ell_1}, \ldots, q^k_{\ell_k})$-well-formedness relation is *transitive*.

Now it is possible to show that a trace whose length exceeds a suitable exponential threshold, induces a shorter, well-formed trace. Such a contraction pattern represents a "basic step" in a contraction process which will allow us to prove the exponential small-model property for $\mathsf{A\overline{A}B\overline{B}}$. Let us consider an $\mathsf{A\overline{A}B\overline{B}}$ formula φ and let $r_1, \ldots, r_k$ be the RE's over $\mathcal{AP}$ in φ. Let $\mathcal{D}^1, \ldots, \mathcal{D}^k$ be the DFAs such that $\mathcal{L}(\mathcal{D}^t) = \mathcal{L}(r_t)$, for $t = 1, \ldots, k$, where $|Q^t| \leq 2^{2^{|r_t|}}$ (see Remark 2). We denote $Q^1 \times \ldots \times Q^k$ by $Q(\varphi)$, and $\mathcal{D}^1, \ldots, \mathcal{D}^k$ by $\mathcal{D}(\varphi)$.

Proposition 10. *Let $\mathcal{K} = (\mathcal{AP}, S, R, \mu, s_0)$ be a finite Kripke structure, φ be an $\mathsf{A\overline{A}B\overline{B}}$ formula with RE's $r_1, \ldots, r_k$ over $\mathcal{AP}$, $\rho \in \mathrm{Trc}_{\mathcal{K}}$ be a trace, and $(q^1, \ldots, q^k) \in Q(\varphi)$. There exists a trace $\pi \in \mathrm{Trc}_{\mathcal{K}}$, which is $(q^1, \ldots, q^k)$-well-formed w.r.t. ρ, such that $|\pi| \leq |S| \cdot 2^{2\sum_{\ell=1}^{k} |r_\ell|}$.*

The next step is to determine some conditions for contracting traces while preserving the equivalence w.r.t. the satisfiability of a considered $\mathsf{A\overline{A}B\overline{B}}$ formula. In the following, we restrict ourselves to formulas in *negation normal form* (abbreviated NNF, a.k.a. *positive normal form*), i.e., formulas where negation is applied only to atomic formulas (regular expressions). Any formula in $\mathsf{A\overline{A}B\overline{B}}$ can be converted (in linear time) into an equivalent one in NNF, having at most double length (by using De Morgan's laws and duality of HS modalities).

For a trace ρ and a formula φ of $\mathsf{A\overline{A}B\overline{B}}$ (in NNF), we fix some special ρ-positions, called *witness positions*, each one corresponding to the minimal prefix of ρ which satisfies a formula ψ occurring in φ as a subformula of the form $\langle \mathrm{B} \rangle \psi$ (provided that $\langle \mathrm{B} \rangle \psi$ is satisfied by ρ). When a contraction is performed in between a pair of *consecutive* witness positions (thus no witness position is ever removed), we get a trace induced by ρ equivalent w.r.t. satisfiability of φ.

Definition 11 (Witness positions). *Let ρ be a trace of $\mathcal{K}$ and φ be a formula of $\mathsf{A\overline{A}B\overline{B}}$. Let us denote by $B(\varphi, \rho)$ the set of subformulas $\langle \mathrm{B} \rangle \psi$ of φ such that $\mathcal{K}, \rho \models \langle \mathrm{B} \rangle \psi$. The* set $Wt(\varphi, \rho)$ of witness positions of ρ for φ *is the* minimal *set of ρ-positions satisfying the following constraint: for each $\langle \mathrm{B} \rangle \psi \in B(\varphi, \rho)$, the smallest ρ-position $i < |\rho|$ such that $\mathcal{K}, \rho^i \models \psi$ belongs to $Wt(\varphi, \rho)$.*[5]

[5] Note that such a ρ-position exists by definition of $B(\varphi, \rho)$.

The cardinality of $B(\varphi,\rho)$ and of $Wt(\varphi,\rho)$ is at most $|\varphi|-1$.

Theorem 12 (Exponential small-model for $\mathsf{A\overline{A}B\overline{B}}$). *Let $\mathcal{K}=(\mathcal{AP},S,R,\mu,s_0)$, $\sigma,\rho \in \mathrm{Trc}_{\mathcal{K}}$, and φ be an $\mathsf{A\overline{A}B\overline{B}}$ formula in NNF, with RE's $r_1,\ldots,r_u$ over $\mathcal{AP}$, such that $\mathcal{K},\sigma\star\rho \models \varphi$. Then, there is $\pi \in \mathrm{Trc}_{\mathcal{K}}$, induced by ρ, such that $\mathcal{K},\sigma\star\pi \models \varphi$ and $|\pi| \leq |S|\cdot(|\varphi|+1)\cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}$.*

Theorem 12 holds in particular if $|\sigma| = 1$, and thus $\sigma\star\rho = \rho$ and $\sigma\star\pi = \pi$. In this case, if $\mathcal{K},\rho \models \varphi$, then $\mathcal{K},\pi \models \varphi$, where π is induced by ρ and $|\pi| \leq |S|\cdot(|\varphi|+1)\cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}$. The more general assertion is needed for technical reasons.

In the following, we will exploit the exponential small-model for $\mathsf{A\overline{A}B\overline{B}}$ and $\mathsf{A\overline{A}E\overline{E}}$ to prove the **PSPACE**-completeness of the MC problem for the two symmetrical fragments. First, we will provide a **PSPACE** MC algorithm for $\mathsf{B\overline{B}}$ (resp., $\mathsf{E\overline{E}}$); then, we will show that the *meets* and *met-by* modalities A and $\overline{\mathsf{A}}$ can be suitably encoded by using regular expressions, and thus they do not increase the complexity of $\mathsf{B\overline{B}}$ (resp., $\mathsf{E\overline{E}}$).

6 PSPACE-completeness of MC for $\mathsf{A\overline{A}B\overline{B}}$

To start with, we describe a **PSPACE** MC algorithm for $\mathsf{B\overline{B}}$ formulas. W.l.o.g., we assume that the processed formulas do not contain occurrences of the universal modalities $[B]$ and $[\overline{B}]$. Moreover, for a formula ψ, we denote by $\mathsf{Subf}_{\langle \mathrm{B}\rangle}(\psi) = \{\varphi \mid \langle \mathrm{B}\rangle\,\varphi \text{ is a subformula of } \psi\}$; Φ represents the overall formula to be checked, while the parametric formula ψ ranges over its subformulas. Due to the result of the previous section, the algorithm can consider only traces having length bounded by the exponential small-model property. Note that an algorithm required to work in polynomial space cannot explicitly store the DFAs for the regular expressions occurring in Φ (their states are *exponentially* many in the length of the associated regular expressions). For this reason, while checking a formula against a trace, the algorithm just stores the *current states* of the computations of the DFAs associated with the regular expressions in Φ, from the respective initial states (in the following such states are denoted—with a little abuse of notation—again by $\mathcal{D}(\Phi)$, and called the *"current configuration" of the DFAs*) and calculates on-the-fly the successor states in the DFAs, once they have read some state of $\mathcal{K}$ used to extend the considered trace (this can be done by exploiting a *succinct* encoding of the NFAs for the reg.expr. of Φ, see Remark 2).

A call to the recursive procedure $\mathtt{Check}(\mathcal{K},\psi,s,G,\mathcal{D}(\Phi))$ (Algorithm 1) checks the satisfiability of a subformula ψ of Φ w.r.t. any trace ρ fulfilling the following conditions: (1) $G \subseteq \mathsf{Subf}_{\langle \mathrm{B}\rangle}(\psi)$ is the set of formulas that hold true on at least a prefix of ρ; (2) after reading $\mu(\rho(1,|\rho|-1))$ the current configuration of the DFAs for the regular expressions of Φ is $\mathcal{D}(\Phi)$; (3) the last state of ρ is s. Intuitively, since the algorithm cannot store the already checked portion of a trace (*whose length could be exponential*), the relevant information is *summarized* in a triple $(G,\mathcal{D}(\Phi),s)$. Hereafter the set of all possible summarizing triples $(\overline{G},\overline{\mathcal{D}(\Phi)},\overline{s})$, where $\overline{G} \subseteq \mathsf{Subf}_{\langle \mathrm{B}\rangle}(\psi)$, $\overline{\mathcal{D}(\Phi)}$ is any current configuration of the DFAs for the regular expressions of Φ, and $\overline{s}$ is a state of $\mathcal{K}$, is denoted by $\mathsf{Conf}(\mathcal{K},\psi)$.

Let us consider in detail the body of the procedure. First $\mathtt{advance}(\mathcal{D}(\Phi),\mu(s))$, invoked at line 2, updates the current configuration of the DFAs after reading

Algorithm 1 $\texttt{Check}(\mathcal{K}, \psi, s, G, \mathcal{D}(\Phi))$

1: **if** $\psi = r$ **then** ◁ *r is a regular expression*
2: **If** the current state of the DFA for r in $\texttt{advance}(\mathcal{D}(\Phi), \mu(s))$ is final **return** $\top$
3: **else return** $\bot$
4: **else if** $\psi = \neg\psi'$ (resp., $\psi = \psi_1 \wedge \psi_2$) **then**
5: Call Check recursively on ψ' (ψ_1, ψ_2) and apply $\neg$ ($\wedge$) to the returned result(s)
6: **else if** $\psi = \langle \mathrm{B} \rangle \psi'$ **then**
7: **If** $\psi' \in G$ **then return** $\top$ **else return** $\bot$
8: **else if** $\psi = \langle \overline{\mathrm{B}} \rangle \psi'$ **then**
9: **for** each $b \in \{1, \ldots, |S| \cdot (2|\psi'| + 1) \cdot 2^{2 \sum_{\ell=1}^{u} |r_\ell|} - 1\}$
and each $(G', \mathcal{D}(\Phi)', s') \in \mathsf{Conf}(\mathcal{K}, \psi)$ **do**◁ *$r_1, \ldots, r_u$ are the reg. expr. of ψ'*
10: **if** $\texttt{Reach}(\mathcal{K}, \psi', (G, \mathcal{D}(\Phi), s), (G', \mathcal{D}(\Phi)', s'), b)$ **and** $\texttt{Check}(\mathcal{K}, \psi', s', G', \mathcal{D}(\Phi)')$ **then**
11: **return** $\top$
12: **return** $\bot$

Algorithm 2 $\texttt{Reach}(\mathcal{K}, \psi, (G_1, \mathcal{D}(\Phi)_1, s_1), (G_2, \mathcal{D}(\Phi)_2, s_2), b)$

1: **if** $b = 1$ **then**
2: **return** $\texttt{Compatible}(\mathcal{K}, \psi, (G_1, \mathcal{D}(\Phi)_1, s_1), (G_2, \mathcal{D}(\Phi)_2, s_2))$
3: **else** ◁ $b \geq 2$
4: $b' \leftarrow \lfloor b/2 \rfloor$
5: **for** each $(G_3, \mathcal{D}(\Phi)_3, s_3) \in \mathsf{Conf}(\mathcal{K}, \psi)$ **do**
6: **if** $\texttt{Reach}(\mathcal{K}, \psi, (G_1, \mathcal{D}(\Phi)_1, s_1), (G_3, \mathcal{D}(\Phi)_3, s_3), b')$ and $\texttt{Reach}(\mathcal{K}, \psi, (G_3, \mathcal{D}(\Phi)_3, s_3), (G_2, \mathcal{D}(\Phi)_2, s_2), b - b')$ **then**
7: **return** $\top$
8: **return** $\bot$

the symbol $\mu(s)$. If ψ is a regular expression r (lines 1–3), we just check whether the (computation of the) DFA associated with r is in a final state (i.e., the summarized trace is accepted). Boolean connectives are easily dealt with recursively (lines 4–5). If ψ has the form $\langle \mathrm{B} \rangle \psi'$ (lines 6–7), then ψ' has to hold over a proper prefix of the summarized trace, namely, ψ' must belong to G.

The only involved case is $\psi = \langle \overline{\mathrm{B}} \rangle \psi'$ (lines 8–12): we have to unravel the Kripke structure $\mathcal{K}$ to find an *extension* ρ' of ρ, summarized by the triple $(G', \mathcal{D}(\Phi)', s')$, satisfying ψ'. The idea is checking whether or not there exists a summarized trace $(G', \mathcal{D}(\Phi)', s')$, suitably extending $(G, \mathcal{D}(\Phi), s)$, namely, such that: (1) $\mathcal{D}(\Phi)'$ and s' are *synchronously* reachable from $\mathcal{D}(\Phi)$ and s, resp.; (2) $G' \supseteq G$ contains all the formulas of $\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi')$ satisfied by some prefixes of the extension; (3) the extension $(G', \mathcal{D}(\Phi)', s')$ satisfies ψ'. In order to check point (1), i.e., synchronous reachability, we can exploit the exponential small-model property and consider only the unravelling of $\mathcal{K}$ starting from s having depth at most $|S| \cdot (2|\psi'| + 1) \cdot 2^{2 \sum_{\ell=1}^{u} |r_\ell|} - 1$[6]. The check of (1) and (2) is performed by the procedure Reach (Algorithm 2), which accepts as input two summarized traces and a bound b on the depth of the unravelling of $\mathcal{K}$. The proposed reachability algorithm is reminiscent of the binary reachability of Savitch's theorem.

Reach proceeds recursively (lines 3–8) by halving at each step the value b of the length bound, until it gets called over two states s_1 and s_2 which are adjacent

[6] The factor 2 in front of $|\psi'|$ is due to the fact that the exponential small-model for $\mathsf{A}\overline{\mathsf{A}}\mathsf{B}\overline{\mathsf{B}}$ requires a formula in NNF.

Algorithm 3 `Compatible`$(\mathcal{K},\psi,(G_1,\mathcal{D}(\Phi)_1,s_1),(G_2,\mathcal{D}(\Phi)_2,s_2))$

1: **if** $(s_1,s_2)\in R$ **and** $\texttt{advance}(\mathcal{D}(\Phi)_1,\mu(s_1))=\mathcal{D}(\Phi)_2$ **and** $G_1\subseteq G_2$ **then**
2: **for** each $\varphi\in(G_2\setminus G_1)$ **do**
3: $G\leftarrow G_1\cap\mathsf{Subf}_{\langle \mathrm{B}\rangle}(\varphi)$
4: **if** $\texttt{Check}(\mathcal{K},\varphi,s_1,G,\mathcal{D}(\Phi)_1)=\bot$ **then**
5: **return** $\bot$
6: **for** each $\varphi\in(\mathsf{Subf}_{\langle \mathrm{B}\rangle}(\psi)\setminus G_2)$ **do**
7: $G\leftarrow G_1\cap\mathsf{Subf}_{\langle \mathrm{B}\rangle}(\varphi)$
8: **if** $\texttt{Check}(\mathcal{K},\varphi,s_1,G,\mathcal{D}(\Phi)_1)=\top$ **then**
9: **return** $\bot$
10: **return** $\top$
11: **else**
12: **return** $\bot$

in a trace. At each halving step, an intermediate summarizing triple is generated to be associated with the split point. At the base of recursion (for $b=1$, lines 1–2), the auxiliary procedure `Compatible` (Algorithm 3) is invoked. At line 1, `Compatible` checks whether there is an edge between s_1 and s_2 ($(s_1,s_2)\in R$), and if, at the considered step, the current configuration of the DFAs $\mathcal{D}(\Phi)_1$ is transformed into the configuration $\mathcal{D}(\Phi)_2$ (i.e., s_2 and $\mathcal{D}(\Phi)_2$ are synchronously reachable from s_1 and $\mathcal{D}(\Phi)_1$). At lines 2–9, `Compatible` checks that each formula φ in $(G_2\setminus G_1)$, where $G_2\supseteq G_1$, is satisfied by a trace summarized by $(G_1,\mathcal{D}(\Phi)_1,s_1)$ (lines 2–5). Intuitively, $(G_1,\mathcal{D}(\Phi)_1,s_1)$ summarizes the maximal prefix of $(G_2,\mathcal{D}(\Phi)_2,s_2)$, and thus a subformula satisfied by a prefix of a trace summarized by $(G_2,\mathcal{D}(\Phi)_2,s_2)$ either belongs to G_1 or it is satisfied by the trace summarized by $(G_1,\mathcal{D}(\Phi)_1,s_1)$. Moreover, (lines 6–9) `Compatible` checks that G_2 is maximal (i.e., no subformula that must be in G_2 has been forgot).

Note that by exploiting this binary reachability technique, the recursion depth of `Reach` is *logarithmic in the length of the trace to be visited, hence it can use only polynomial space*. Theorem 13 establishes the soundness of `Check`.

Theorem 13. *Let Φ be a $\mathsf{B\overline{B}}$ formula, ψ be a subformula of Φ, and $\rho\in\mathrm{Trc}_{\mathcal{K}}$ be a trace with $s=\mathrm{lst}(\rho)$. Let G be the subset of formulas in $\mathsf{Subf}_{\langle \mathrm{B}\rangle}(\psi)$ that hold on some proper prefix of ρ. Let $\mathcal{D}(\Phi)$ be the current configuration of the DFAs associated with the regular expressions in Φ after reading $\mu(\rho(1,|\rho|-1))$. Then $\texttt{Check}(\mathcal{K},\psi,s,G,\mathcal{D}(\Phi))=\top\iff\mathcal{K},\rho\models\psi$.*

Finally, the main MC procedure for $\mathsf{B\overline{B}}$ formulas is reported in Algorithm 4: `CheckAux`$(\mathcal{K},\Phi)$ starts by constructing the NFAs and the initial states of the DFAs for the regular expressions of Φ. Then `CheckAux` invokes the procedure `Check` two times: the former to check the special case of the trace s_0 (consisting of the initial state of $\mathcal{K}$ only), and the latter for considering any right-extensions of s_0 (i.e., all the initial traces having length at least 2).

Theorem 14. *Let $\mathcal{K}=(\mathcal{AP},S,R,\mu,s_0)$ be a finite Kripke structure, and Φ be a $\mathsf{B\overline{B}}$ formula. Then $\texttt{CheckAux}(\mathcal{K},\Phi)$ returns $\top$ if and only if $\mathcal{K}\models\Phi$.*

Corollary 15. *The MC problem for $\mathsf{B\overline{B}}$ formulas over finite Kripke structures is in* **PSPACE**.

Algorithm 4 $\texttt{CheckAux}(\mathcal{K}, \Phi)$

1: $\texttt{create}(\mathcal{D}(\Phi)_0)\triangleleft$ *Creates the (succinct) NFAs and the initial states of the DFAs for all the regular expressions in* Φ
2: **If** $\texttt{Check}(\mathcal{K}, \neg\Phi, s_0, \emptyset, \mathcal{D}(\Phi)_0)$ **or** $\texttt{Check}(\mathcal{K}, \langle\overline{\text{B}}\rangle\, \neg\Phi, s_0, \emptyset, \mathcal{D}(\Phi)_0)$ **then return** $\bot$
3: **else return** $\top$

Proof. The procedure `CheckAux` decides the problem using *polynomial work space* due to the following facts: (i) the number of simultaneously active recursive calls of `Check` is $O(|\Phi|)$ (depending on the depth of Φ); (ii) for any call of `Check` the used space (in bits) is $O\Big(\big(|\Phi|+|S|+\sum_{\ell=1}^{u}|r_\ell|+\log(|S|\cdot|\Phi|\cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}\big)_{(1)}+ \big(|\Phi|+|S|+\sum_{\ell=1}^{u}|r_\ell|\big)_{(2)}\cdot\log(|S|\cdot|\Phi|\cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}\big)_{(3)}\Big)$ where $r_1,\ldots,r_u$ are the regular expressions of Φ, and S the states of $\mathcal{K}$. In particular, (1) $O(\log(|S|\cdot|\Phi|\cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}))$ bits are used for the bound b on the trace length, (3) for *each subformula* $\langle\overline{\text{B}}\rangle\,\psi'$ of Φ at most $O(\log(|S|\cdot|\Phi|\cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}))$ recursive calls of `Reach` may be simultaneously active (the recursion depth of `Reach` is logarithmic in b), and (2) each call of `Reach` requires $O(|\Phi|+|S|+\sum_{\ell=1}^{u}|r_\ell|)$ bits. □

Finally, since a Kripke structure can be unravelled against the direction of its edges, and any language $\mathcal{L}$ is regular iff $\mathcal{L}^{\text{Rev}}=\{w(|w|)\cdots w(1)\mid w\in\mathcal{L}\}$ is, the algorithm can be easily modified to deal with the symmetrical fragment $\mathsf{E}\overline{\mathsf{E}}$.

Let us now focus on $\mathsf{A}\overline{\mathsf{A}}\mathsf{B}\overline{\mathsf{B}}$. `CheckAux` can be used iteratively as a basic engine to check formulas Φ of $\mathsf{A}\overline{\mathsf{A}}\mathsf{B}\overline{\mathsf{B}}$: at each iteration, we select an occurrence of a subformula of Φ, either of the form $\langle\text{A}\rangle\,\psi$ or $\langle\overline{\text{A}}\rangle\,\psi$, without *internal* occurrences of $\langle\text{A}\rangle$ and $\langle\overline{\text{A}}\rangle$. For such an occurrence, say $\langle\text{A}\rangle\,\psi$ ($\langle\overline{\text{A}}\rangle\,\psi$ is symmetric), we compute the set $S_{\langle\text{A}\rangle\,\psi}$ of states of $\mathcal{K}$ s.t., for any $\rho\in\text{Trc}_{\mathcal{K}}$, $\mathcal{K},\rho\models\langle\text{A}\rangle\,\psi$ iff $\text{lst}(\rho)\in S_{\langle\text{A}\rangle\,\psi}$. To this aim we run $\texttt{CheckAux}(\mathcal{K},\neg\psi)$ using each $s\in S$ as the initial state (in place of s_0): we have $s\in S_{\langle\text{A}\rangle\,\psi}$ iff the procedure returns $\bot$. Then we replace $\langle\text{A}\rangle\,\psi$ in Φ with a fresh reg. expr. $r_{\langle\text{A}\rangle\,\psi}:=\top^*\cdot\big(\bigcup_{s'\in S_{\langle\text{A}\rangle\,\psi}}q_{s'}\big)$—where $q_{s'}$ is an auxiliary letter labeling $s'\in S$ only—obtaining a formula Φ'. If Φ' is in $\mathsf{B}\overline{\mathsf{B}}$ the conversion is completed, otherwise we proceed with another iteration.

Finally, the pure propositional fragment Prop can be proved **PSPACE**-hard by a reduction from the **PSPACE**-complete *universality problem for regular expressions*: such lower bound immediately propagates to all other HS fragments.

Theorem 16. *The MC problem for formulas of any (proper or improper) subfragment of* $\mathsf{A}\overline{\mathsf{A}}\mathsf{B}\overline{\mathsf{B}}$ *(and* $\mathsf{A}\overline{\mathsf{A}}\mathsf{E}\overline{\mathsf{E}}$*) on finite Kripke structures is* **PSPACE***-complete.*

7 Conclusions

In this paper, we have investigated the MC problem for HS and two large fragments of it, $\mathsf{A}\overline{\mathsf{A}}\mathsf{B}\overline{\mathsf{B}}$ and $\mathsf{A}\overline{\mathsf{A}}\mathsf{E}\overline{\mathsf{E}}$, defining interval labelling via regular expressions. The approach, stemming from [12], generalizes both the one of [14] (which assumes the homogeneity principle) and of [10, 11] (where labeling is endpoint-based). MC turns out to be non-elementarily decidable and **EXPSPACE**-hard for full HS (the hardness follows from that of BE under homogeneity [3]), and **PSPACE**-complete for $\mathsf{A}\overline{\mathsf{A}}\mathsf{B}\overline{\mathsf{B}}$, $\mathsf{A}\overline{\mathsf{A}}\mathsf{E}\overline{\mathsf{E}}$, and all their sub-fragments.

Future work will focus on the fragments $\mathsf{A\overline{A}B\overline{BE}}$, $\mathsf{A\overline{A}E\overline{BE}}$, and $\mathsf{A\overline{AB}\overline{E}}$, which have been proved to be in **EXPSPACE** (the first two) and **PSPACE**-complete (the third one) under the homogeneity assumption [15, 16], as well as on the problem of determining the exact complexity of MC for full HS. In addition, we will study the MC problem for HS over *visibly pushdown systems* (VPS), in order to deal with recursive programs and infinite state systems.

References

1. Allen, J.F.: Maintaining knowledge about temporal intervals. Comm. of the ACM 26(11), 832–843 (1983)
2. Baier, C., Katoen, J.: Principles of model checking. MIT Press (2008)
3. Bozzelli, L., Molinari, A., Montanari, A., Peron, A., Sala, P.: Interval Temporal Logic Model Checking: the Border Between Good and Bad HS Fragments. In: IJCAR. pp. 389–405. LNAI 9706 (2016)
4. Bozzelli, L., Molinari, A., Montanari, A., Peron, A., Sala, P.: Interval vs. Point Temporal Logic Model Checking: an Expressiveness Comparison. In: FSTTCS (2016)
5. Bozzelli, L., Molinari, A., Montanari, A., Peron, A., Sala, P.: Model Checking the Logic of Allen's Relations Meets and Started-by is $\mathbf{P^{NP}}$-Complete. In: GandALF. pp. 76–90 (2016)
6. Bresolin, D., Della Monica, D., Goranko, V., Montanari, A., Sciavicco, G.: The dark side of interval temporal logic: marking the undecidability border. Annals of Mathematics and Artificial Intelligence 71(1-3), 41–83 (2014)
7. Esparza, J., Hansel, D., Rossmanith, P., Schwoon, S.: Efficient algorithms for model checking pushdown systems. In: CAV. pp. 232–247 (2000)
8. Halpern, J.Y., Shoham, Y.: A propositional modal logic of time intervals. J. of the ACM 38(4), 935–962 (1991)
9. Kupferman, O., Piterman, N., Vardi, M.Y.: From liveness to promptness. Formal Methods in System Design 34(2), 83–103 (2009)
10. Lomuscio, A., Michaliszyn, J.: An epistemic Halpern-Shoham logic. In: IJCAI. pp. 1010–1016 (2013)
11. Lomuscio, A., Michaliszyn, J.: Decidability of model checking multi-agent systems against a class of EHS specifications. In: ECAI. pp. 543–548 (2014)
12. Lomuscio, A., Michaliszyn, J.: Model checking multi-agent systems against epistemic HS specifications with regular expressions. In: KR. pp. 298–308 (2016)
13. Marcinkowski, J., Michaliszyn, J.: The undecidability of the logic of subintervals. Fundamenta Informaticae 131(2), 217–240 (2014)
14. Molinari, A., Montanari, A., Murano, A., Perelli, G., Peron, A.: Checking interval properties of computations. Acta Informatica pp. 587–619 (2016)
15. Molinari, A., Montanari, A., Peron, A.: Complexity of ITL model checking: some well-behaved fragments of the interval logic HS. In: TIME. pp. 90–100 (2015)
16. Molinari, A., Montanari, A., Peron, A.: A model checking procedure for interval temporal logics based on track representatives. In: CSL. pp. 193–210 (2015)
17. Molinari, A., Montanari, A., Peron, A., Sala, P.: Model Checking Well-Behaved Fragments of HS: the (Almost) Final Picture. In: KR. pp. 473–483 (2016)
18. Montanari, A.: Interval temporal logics model checking. In: TIME. p. 2 (2016)
19. Moszkowski, B.: Reasoning About Digital Circuits. Ph.D. thesis, Stanford University, Stanford, CA (1983)
20. Roeper, P.: Intervals and tenses. J. of Philosophical Logic 9, 451–469 (1980)
21. Venema, Y.: Expressiveness and completeness of an interval tense logic. Notre Dame J. of Formal Logic 31(4), 529–547 (1990)

A Appendix

A.1 Completion of the proof of Proposition 5

Construction for the language $\langle \mathrm{E} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$. Let us consider the NFA $\mathcal{A}_{\langle \mathrm{E} \rangle}$ over S given by $\mathcal{A}_{\langle \mathrm{E} \rangle} = (S, (M \cup \{q_0'\}) \times S, \{q_0'\} \times S, \delta', F)$, where $q_0' \notin M$ is a fresh main state and for all $(q, s) \in (M \cup \{q_0'\}) \times S$ and $s' \in S$, $\delta'((q, s), s') = \emptyset$, if $s' \neq s$, and $\delta((q, s), s)$ is defined as follows:

$$\delta((q,s),s) = \begin{cases} \delta((q,s),s) & \text{if } q \neq q_0' \\ (\{q_0'\} \times R(s)) \cup \{(q_0, s') \in Q_0 \mid s' \in R(s)\} & \text{otherwise.} \end{cases}$$

Starting from an initial state (q_0', s), the automaton $\mathcal{A}_{\langle \mathrm{E} \rangle}$ either remains in a state whose main component is q_0', or moves to an initial state (q_0, s') of $\mathcal{A}$, ensuring at the same time that the portion of the input read so far is faithful to the evolution of $\mathcal{K}$. From the state (q_0, s'), $\mathcal{A}_{\langle \mathrm{E} \rangle}$ simulates the behavior of $\mathcal{A}$. Formally, since $\mathcal{A}$ is a $\mathcal{K}$-NFA, by construction it easily follows that $\mathcal{A}_{\langle \mathrm{E} \rangle}$ is a $\mathcal{K}$-NFA which accepts the set of traces of $\mathcal{K}$ having a non-empty proper suffix in $\mathcal{L}(\mathcal{A})$. Hence, $\mathcal{L}(\mathcal{A}_{\langle \mathrm{E} \rangle}) = \langle \mathrm{E} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$.

Construction for the language $\langle \overline{\mathrm{E}} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$. Let us consider the NFA $\mathcal{A}_{\langle \overline{\mathrm{E}} \rangle}$ over S given by $\mathcal{A}_{\langle \overline{\mathrm{E}} \rangle} = (S, (M \cup \{q_{acc}\}) \times S, Q_0', \delta', \{q_{acc}\} \times S)$, where $q_{acc} \notin M$ is a fresh main state, and Q_0' and δ' are defined as follows:

- the set Q_0' of initial states is the set of states (q, s) of $\mathcal{A}$ such that there is a run of $\mathcal{A}$ from some initial state to (q, s) over some non-empty word.
- For all $(q, s) \in (M \cup \{q_{acc}\}) \times S$ and $s' \in S$, $\delta'((q, s), s') = \emptyset$ if $s' \neq s$, and $\delta'((q, s), s)$ is as follows:

$$\delta'((q,s),s) = \begin{cases} \delta((q,s),s) \cup \bigcup_{(q',s') \in F \cap \delta((q,s),s)} \{(q_{acc}, s')\} & \text{if } q \in M \\ \emptyset & \text{if } q = q_{acc}. \end{cases}$$

Note that the set Q_0' can be computed in time polynomial in the size of $\mathcal{A}$. Since $\mathcal{A}_{\langle \overline{\mathrm{E}} \rangle}$ essentially simulates $\mathcal{A}$, and $\mathcal{A}$ is a $\mathcal{K}$-NFA, by construction we easily obtain that $\mathcal{A}_{\langle \overline{\mathrm{E}} \rangle}$ is a $\mathcal{K}$-NFA which accepts the set of words over S which are non-empty proper suffixes of words in $\mathcal{L}(\mathcal{A})$. Thus, since $\mathcal{A}$ is a $\mathcal{K}$-NFA, we obtain that $\mathcal{L}(\mathcal{A}_{\langle \overline{\mathrm{E}} \rangle}) = \langle \overline{\mathrm{E}} \rangle_{\mathcal{K}}(\mathcal{L}(\mathcal{A}))$. □

A.2 Completion of the proof of Proposition 6

Union. Let $\mathcal{A} = (S, M \times S, Q_0, \delta, F)$ and $\mathcal{A}' = (S, M' \times S, Q_0', \delta', F')$ be the given $\mathcal{K}$-NFAs. W.l.o.g., we assume that $M \cap M' = \emptyset$. Let us consider the NFA $\mathcal{A}_{\cup}$ over S given by $\mathcal{A}_{\cup} = (S, (M \cup M') \times S, Q_0 \cup Q_0', \delta'', F \cup F')$, where for all $(q, s) \in (M \cup M') \times S$ and $s' \in S$, $\delta''((q, s), s') = \emptyset$ if $s' \neq s$, and $\delta''((q, s), s)$ is defined as follows:

$$\delta''((q,s),s) = \begin{cases} \delta((q,s),s) & \text{if } q \in M \\ \delta'((q,s),s) & \text{if } q \in M'. \end{cases}$$

Correctness of the construction trivially follows.

Complementation. Recall that $\mathcal{A} = (S, M \times S, Q_0, \delta, F)$. Let n be the number of main states of $\mathcal{A}$. First, we need a preliminary construction. Let us consider the NFA $\mathcal{A}'' = (S, (M \cup \{q_{acc}\}) \times S, Q_0, \delta'', \{q_{acc}\} \times S)$, where $q_{acc} \notin M$ is a fresh main state, and for all $(q, s) \in (M \cup \{q_{acc}\}) \times S$ and $s' \in s$, $\delta''((q, s), s') = \emptyset$ if $s' \neq s$, and $\delta''((q, s), s)$ is defined as follows:

$$\delta''((q,s),s) = \begin{cases} \delta((q,s),s) \cup (\{q_{acc}\} \times S) & \text{if } q \in M \text{ and } \delta((q,s),s) \cap F \neq \emptyset \\ \delta((q,s),s) & \text{if } q \in M \text{ and } \delta((q,s),s) \cap F = \emptyset \\ \emptyset & \text{if } q = q_{acc}. \end{cases}$$

Note that $\mathcal{A}''$ is *not* a $\mathcal{K}$-NFA. However, $\mathcal{L}(\mathcal{A}'') = \mathcal{L}(\mathcal{A})$.

Next we show that it is possible to construct in time $2^{O(n)}$ a *weak* $\mathcal{K}$-NFA $\mathcal{A}_c$ with 2^{n+1} main states accepting $(\mathrm{Trc}_{\mathcal{K}} \setminus \mathcal{L}(\mathcal{A}'')) \cup \{\varepsilon\}$, where a *weak* $\mathcal{K}$-NFA is a $\mathcal{K}$-NFA but the requirement that the empty word ε is not accepted is relaxed. Thus, since a weak $\mathcal{K}$-NFA can be easily converted into an equivalent $\mathcal{K}$-NFA by using an additional main state and $\mathcal{L}(\mathcal{A}'') = \mathcal{L}(\mathcal{A})$, the result follows. Let $\tilde{M} = M \cup \{q_{acc}\}$. Then, the weak $\mathcal{K}$-NFA $\mathcal{A}_c$ is given by $\mathcal{A}_c = (S, 2^{\tilde{M}} \times S, Q_{0,c}, \delta_c, F_c)$, where $Q_{0,c}$, δ_c, and F_c are defined as follows:

- $Q_{0,c} = \{(P, s) \in 2^M \times S \mid P = \{q \in M \mid (q, s) \in Q_0\}\}$;
- for all $(P, s) \in 2^{\tilde{M}} \times S$ and $s' \in S$, $\delta_c((P, s), s') = \emptyset$ if $s' \neq s$, and $\delta_c((P, s), s)$ is given by

$$\bigcup_{s' \in R(s)} \left\{ (\{q' \in \tilde{M} \mid (q', s') \in \bigcup_{p \in P} \delta''(p, s)\}, s') \right\};$$

- $F_c = \{(P, s) \in 2^M \times S\}$.

By construction, $\mathcal{A}_c$ is a weak $\mathcal{K}$-NFA. Hence $\mathcal{A}_c$ does not accept words in $S^+ \setminus \mathrm{Trc}_{\mathcal{K}}$. Moreover, by construction $Q_{0,c} \subseteq F$. Hence $\varepsilon \in \mathcal{L}(\mathcal{A}_c)$. Let $\rho \in \mathrm{Trc}_{\mathcal{K}}$ with $|\rho| = k$. It remains to show that $\rho \in \mathcal{L}(\mathcal{A}'')$ if and only if $\rho \notin \mathcal{L}(\mathcal{A}_c)$.

First, let $\rho \in \mathcal{L}(\mathcal{A}'')$. We show that $\rho \notin \mathcal{L}(\mathcal{A}_c)$. We assume the contrary and derive a contradiction. Hence, there is a run of $\mathcal{A}_c$ over ρ of the form $(P_0, s_0), \ldots, (P_k, s_k)$ such that $(P_0, s_0) \in Q_{0,c}$ and $(P_k, s_k) \in F_c$. Hence $q_{acc} \notin P_k$. By construction, $P_0 = \{q \in M \mid (q, s_0) \in Q_0\}$, and for all $i \in [0, k-1]$, $s_i = \rho(i)$ and $P_{i+1} = \{p \in \tilde{M} | (p, s_{i+1}) \in \delta''(q, s_i)$ for some $q \in P_i\}$. Since $\rho \in \mathcal{L}(\mathcal{A}'')$, there is $s \in S$, $(q_0, s_0) \in Q_0$ and an accepting run of $\mathcal{A}''$ over ρ of the form $(q_0, s_0), \ldots, (q_{k-1}, s_{k-1}), (q_k, s)$ where $q_k = q_{acc}$. By definition of the transition function of $\mathcal{A}''$, we can also assume that $s = s_k$. It follows that $q_i \in P_i$ for all $i \in [0, k]$, which is a contradiction since $q_{acc} \notin P_k$. Therefore, $\rho \notin \mathcal{L}(\mathcal{A}_c)$.

For the converse direction, let $\rho \notin \mathcal{L}(\mathcal{A}_c)$. We need to show that $\rho \in \mathcal{L}(\mathcal{A}'')$. By construction, there is some run of $\mathcal{A}_c$ over ρ starting from an initial state (recall that $R(s) \neq \emptyset$ for all $s \in S$). Moreover, each of such runs is of the form $(P_0, s_0), \ldots, (P_k, s_k)$ such that $P_0 = \{q \in M \mid (q, s_0) \in Q_0\}$, $q_{acc} \in P_k$, and for all $i \in [0, k-1]$, $s_i = \rho(i)$ and $P_{i+1} = \{p \in \tilde{M} | (p, s_{i+1}) \in \delta(q, s_i)$ for some $q \in P_i\}$. It easily follows that there is an accepting run of $\mathcal{A}''$ over ρ from some initial state in $P_0 \times \{s_0\}$. Hence, the result follows.

This concludes the proof of Proposition 6. □

A.3 Proof of Proposition 10

Proof. Let $\rho \in \mathrm{Trc}_{\mathcal{K}}$ with $|\rho| = n$. If $n \leq |S| \cdot 2^{2\sum_{\ell=1}^{k}|r_\ell|}$, the thesis trivially holds. Thus, let us assume $n > |S| \cdot 2^{2\sum_{\ell=1}^{k}|r_\ell|}$. We show that there exists a trace which is $(q^1, \ldots, q^k)$-well-formed w.r.t. ρ, whose length is smaller than n. The number of possible (joint) configurations of the DFAs $\mathcal{D}(\varphi)$ is (at most) $|Q(\varphi)| \leq 2^{2|r_1|} \ldots 2^{2|r_k|} = 2^{2\sum_{\ell=1}^{k}|r_\ell|}$. Since $n > |S| \cdot 2^{2\sum_{\ell=1}^{k}|r_\ell|}$, there exists some state $s \in S$ occurring in ρ at least twice in the ρ-positions say $1 \leq l_1 < l_2 \leq |\rho|$, such that $\mathcal{D}^t_{q^t}(\mu(\rho^{l_1})) = \mathcal{D}^t_{q^t}(\mu(\rho^{l_2}))$, for all $t = 1, \ldots, k$. Let us consider $\pi = \rho(1, l_1) \star \rho(l_2, n)$. It is easy to see that $\pi \in \mathrm{Trc}_{\mathcal{K}}$, as $\rho(l_1) = \rho(l_2)$, and $|\pi| < n$. Moreover, π is $(q^1, \ldots, q^k)$-well-formed w.r.t. ρ (the corresponding positions are $i_j = j$ if $j \leq l_1$, and $i_j = j + (l_2 - l_1)$ otherwise). Now, if $|\pi| \leq |S| \cdot 2^{2\sum_{\ell=1}^{k}|r_\ell|}$, the thesis holds. Otherwise, the same basic step can be iterated a finite number of times: the thesis follows by transitivity of $(q^1, \ldots, q^k)$-well-formedness. □

A.4 Proof of Theorem 12

Proof. Let $Wt(\varphi, \sigma \star \rho)$ be the set of witness positions of $\sigma \star \rho$ for φ. Let $\{i_1, \ldots, i_k\}$ be the ordering of $Wt(\varphi, \sigma \star \rho)$ such that $i_1 < \ldots < i_k$. Let $i_0 = 1$ and $i_{k+1} = |\sigma \star \rho|$. Hence, $1 = i_0 \leq i_1 < \ldots < i_k < i_{k+1} = |\sigma \star \rho|$.

If the length of ρ is at most $|S| \cdot (|\varphi| + 1) \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}$, the thesis trivially holds. Let us assume that $|\rho| > |S| \cdot (|\varphi| + 1) \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}$. We show that there exists a trace π induced by ρ, with $|\pi| < |\rho|$, such that $\mathcal{K}, \sigma \star \pi \models \varphi$.

W.l.o.g., we can assume that $i_0 \leq i_1 < \ldots < i_{j-1}$, for some $j \geq 1$, are σ-positions (while $i_j < \ldots < i_{k+1}$ are $(\sigma \star \rho)$-positions not in σ). We claim that either (i) there exists $t \in [j, k]$ such that $i_{t+1} - i_t > |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}$ or (ii) $|(\sigma \star \rho)(|\sigma|, i_j)| > |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}$. By way of contradiction, suppose that neither (i) nor (ii) holds. We need to distinguish two cases. If $\sigma \star \rho = \rho$, then $|\rho| = (i_{k+1} - i_0) + 1 \leq (k + 1) \cdot |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|} + 1$; otherwise ($|\rho| < |\sigma \star \rho|$), $|\rho| = (i_{k+1} - i_j) + |(\sigma \star \rho)(|\sigma|, i_j)| \leq k \cdot |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|} + |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|} \leq (k+1) \cdot |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}$. The contradiction follows since $(k+1) \cdot |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|} + 1 \leq |\varphi| \cdot |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|} + 1 \leq |S| \cdot (|\varphi| + 1) \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}$.

Let us define $(\alpha, \beta) = (i_t, i_{t+1})$ in case (i), and $(\alpha, \beta) = (|\sigma|, i_j)$ in case (ii). Moreover let $\rho' = \rho(\alpha, \beta)$. In both the cases, we have $|\rho'| > |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|}$. By Proposition 10, there exists a trace π' of $\mathcal{K}$, $(q^1, \cdots, q^u)$-well-formed with respect to ρ', such that $|\pi'| \leq |S| \cdot 2^{2\sum_{\ell=1}^{u}|r_\ell|} < |\rho'|$, where we choose $q^x = \mathcal{D}^x(\mu((\sigma \star \rho)^{\alpha-1}))$ for $x = 1, \ldots, u$ (as a particular case we set q_x as the initial state of $\mathcal{D}^x$ if $\alpha = 1$). Let π be the trace induced by ρ obtained by replacing the subtrace ρ' of ρ with π'. Since $|\pi| < |\rho|$, it remains to prove that $\mathcal{K}, \sigma \star \pi \models \varphi$.

Let us denote $\sigma \star \pi$ by $\overline{\pi}$ and $\sigma \star \rho$ by $\overline{\rho}$. Moreover, let $H : [1, |\overline{\pi}|] \to [1, |\overline{\rho}|]$ be the function mapping positions of $\overline{\pi}$ into positions of $\overline{\rho}$ in this way: positions "outside" π' (i.e., outside the interval $[\alpha, \alpha + |\pi'| - 1]$) are mapped into their original position in $\overline{\rho}$; positions "inside" π' (i.e., in $[\alpha, \alpha + |\pi'| - 1]$) are mapped to the corresponding position in ρ' (exploiting well-formedness of π' w.r. to ρ').

Formally, H is defined as:

$$H(m) = \begin{cases} m & \text{if} \quad m < \alpha \\ \alpha + \ell_{m-\alpha+1} - 1 & \text{if} \quad \alpha \leq m < \alpha + |\pi'| \\ m + (|\rho'| - |\pi'|) & \text{if} \quad m \geq \alpha + |\pi'| \end{cases} \tag{1}$$

where ℓ_m is the ρ'-position corresponding to the π'-position m. It is easy to check that H satisfies the following properties:

1. H is strictly monotonic, i.e., for all $j, j' \in [1, |\overline{\pi}|]$, $j < j'$ iff $H(j) < H(j')$;
2. for all $j \in [1, |\overline{\pi}|]$, $\overline{\pi}(j) = \overline{\rho}(H(j))$;
3. $H(1) = 1$ and $H(|\overline{\pi}|) = |\overline{\rho}|$;
4. $Wt(\varphi, \overline{\rho}) \subseteq \{H(j) \mid j \in [1, |\overline{\pi}|]\}$;
5. for each $j \in [1, |\overline{\pi}|]$ and $x = 1, \ldots, u$, $\mathcal{D}^x(\mu(\overline{\pi}^j)) = \mathcal{D}^x(\mu(\overline{\rho}^{H(j)}))$.

We only comment on Property 5. The property holds for $j \in [1, \alpha - 1]$, as $\overline{\pi}^j = \overline{\rho}^{H(j)} = \overline{\rho}^j$. For $j \in [\alpha, \alpha + |\pi'| - 1]$, $\mathcal{D}^x(\mu(\overline{\pi}^j)) = \mathcal{D}^x(\mu(\overline{\rho}^{H(j)}))$ follows from the well-formedness hypothesis. Finally, being $\overline{\rho}(\beta, |\overline{\rho}|) = \overline{\pi}(\alpha + |\pi'| - 1, |\overline{\pi}|)$ and $\mathcal{D}^x(\mu(\overline{\pi}^{\alpha+|\pi'|-1})) = \mathcal{D}^x(\mu(\overline{\rho}^{\beta}))$, the property holds also for $j \in [\alpha + |\pi'|, |\overline{\pi}|]$.

The statement $\mathcal{K}, \overline{\pi} \models \varphi$ is an immediate consequence of the following claim, considering that $H(|\overline{\pi}|) = |\overline{\rho}|$, $\mathcal{K}, \overline{\rho} \models \varphi$, $\overline{\rho}^{|\overline{\rho}|} = \overline{\rho}$, and $\overline{\pi}^{|\overline{\pi}|} = \overline{\pi}$.

Claim. For all $j \in [1, |\overline{\pi}|]$, all subformulas ψ of φ, and all $\xi \in \mathrm{Trc}_{\mathcal{K}}$, if $\mathcal{K}, \overline{\rho}^{H(j)} \star \xi \models \psi$ then $\mathcal{K}, \overline{\pi}^j \star \xi \models \psi$.

Proof. Assume that $\mathcal{K}, \overline{\rho}^{H(j)} \star \xi \models \psi$. Note that $\overline{\rho}^{H(j)} \star \xi$ is defined iff $\overline{\pi}^j \star \xi$ is defined. We prove by induction on the structure of ψ that $\mathcal{K}, \overline{\pi}^j \star \xi \models \psi$. Since φ is in NNF, only the following cases can occur:

- $\psi = r_t$ or $\psi = \neg r_t$ where r_t is some RE over $\mathcal{AP}$. By Property 5 of H, $\mathcal{D}^t(\mu(\overline{\pi}^j)) = \mathcal{D}^t(\mu(\overline{\rho}^{H(j)}))$, thus $\mathcal{D}^t(\mu(\overline{\pi}^j \star \xi)) = \mathcal{D}^t(\mu(\overline{\rho}^{H(j)} \star \xi))$. It follows that $\mathcal{K}, \overline{\pi}^j \star \xi \models r_t$ iff $\mathcal{K}, \overline{\rho}^{H(j)} \star \xi \models r_t$, and the result holds.
- $\psi = \theta_1 \wedge \theta_2$ or $\psi = \theta_1 \vee \theta_2$, for some $\mathsf{A\overline{A}B\overline{B}}$ formulas θ_1 and θ_2. The result holds by the inductive hypothesis.
- $\psi = [B]\theta$. We need to show that for each proper prefix η of $\overline{\pi}^j \star \xi$, $\mathcal{K}, \eta \models \theta$. We distinguish two cases:
  - η is *not* a proper prefix of $\overline{\pi}^j$. Hence, η is of the form $\overline{\pi}^j \star \xi^h$ for some $h \in [1, |\xi| - 1]$. Since $\mathcal{K}, \overline{\rho}^{H(j)} \star \xi \models [B]\theta$, then $\mathcal{K}, \overline{\rho}^{H(j)} \star \xi^h \models \theta$. By the inductive hypothesis, $\mathcal{K}, \overline{\pi}^j \star \xi^h \models \theta$.
  - η is a proper prefix of $\overline{\pi}^j$. Hence, $\eta = \overline{\pi}^h$ for some $h \in [1, j - 1]$. By Property 1 of H, $H(h) < H(j)$, and since $\mathcal{K}, \overline{\rho}^{H(j)} \star \xi \models [B]\theta$, we have that $\mathcal{K}, \overline{\rho}^{H(h)} \models \theta$. By the inductive hypothesis, $\mathcal{K}, \overline{\pi}^h \models \theta$.

  Therefore, $\mathcal{K}, \overline{\pi}^j \star \xi \models [B]\theta$.
- $\psi = \langle \mathrm{B} \rangle \theta$. We need to show that there exists a proper prefix of $\overline{\pi}^j \star \xi$ satisfying θ. Since $\mathcal{K}, \overline{\rho}^{H(j)} \star \xi \models \psi$, there exists a proper prefix η' of $\overline{\rho}^{H(j)} \star \xi$ such that $\mathcal{K}, \eta' \models \theta$. We distinguish two cases:
  - η' is *not* a proper prefix of $\overline{\rho}^{H(j)}$. Hence, η' is of the form $\overline{\rho}^{H(j)} \star \xi^h$ for some $h \in [1, |\xi| - 1]$. By the inductive hypothesis, $\mathcal{K}, \overline{\pi}^j \star \xi^h \models \theta$, and $\mathcal{K}, \overline{\pi}^j \star \xi \models \langle \mathrm{B} \rangle \theta$.

- η' is a proper prefix of $\overline{\rho}^{H(j)}$. Hence, $\eta' = \overline{\rho}^{i}$ for some $i \in [1, H(j)-1]$, and $\mathcal{K}, \overline{\rho}^{i} \models \theta$. Let i' be the smallest position of $\overline{\rho}$ such that $\mathcal{K}, \overline{\rho}^{i'} \models \theta$. Hence $i' \leq i$ and, by Definition 11, $i' \in Wt(\varphi, \overline{\rho})$. By Property 4 of H, $i' = H(h)$ for some $\overline{\pi}$-position h. Since $H(h) < H(j)$, it holds that $h < j$ (Property 1). By the inductive hypothesis, $\mathcal{K}, \overline{\pi}^{h} \models \theta$, and $\mathcal{K}, \overline{\pi}^{j} \star \xi \models \langle \mathrm{B} \rangle\, \theta$.

– $\psi = [\overline{B}]\theta$ or $\psi = \langle \overline{\mathrm{B}} \rangle\, \theta$. The result holds as a direct consequence of the inductive hypothesis.

– $\psi = [A]\theta$, $\psi = \langle \mathrm{A} \rangle\, \theta$, $\psi = [\overline{A}]\theta$ or $\psi = \langle \overline{\mathrm{A}} \rangle\, \theta$. Since $\overline{\pi}^{j} \star \xi$ and $\overline{\rho}^{H(j)} \star \xi$ start at the same state and lead to the same state (by Properties 2 and 3 of H), the result trivially follows, concluding the proof of the claim. □

We have proved that $\mathcal{K}, \overline{\pi} \models \varphi$, with $|\pi| < |\rho|$. If $|\pi| \leq |S| \cdot (|\varphi|+1) \cdot 2^{2 \sum_{\ell=1}^{u} |r_\ell|}$, the thesis hold. Otherwise, we can iterate the above contraction (a finite number of times) until the bound is achieved. □

A.5 The exponential small-model is strict: an example

The following example shows that the exponential small-model is strict, that is, there exists a formula and a Kripke structure, such that the shortest trace satisfying the formula has exponential length in the size of the formula. This is the case even for pure propositional formulas.

Example 17. Let pr_i be the i-th smallest prime. It is well-known that $pr_i \in O(i \log i)$. Let $w^{\otimes k}$ denote the string obtained by concatenating k times w. Let us fix some $n \in \mathbb{N}$, and let $\mathcal{K} = (\{p\}, \{s\}, R, \mu, s)$ be the trivial Kripke structure having only one state with a self-loop, where $R = \{(s, s)\}$, and $\mu(s) = \{p\}$. The shortest trace satisfying $\psi = \bigwedge_{i=1}^{n} (p^{\otimes (pr_i)})^*$ is $\rho = s^{\otimes (pr_1 \cdots pr_n)}$, since its length is the least common multiple of $pr_1, \ldots, pr_n$, which is indeed $pr_1 \cdots pr_n$. It is immediate to check that the length of ψ is $O(n \cdot pr_n) = O(n^2 \log n)$. On the other hand, the length of ρ is $pr_1 \cdots pr_n \geq 2^n$. □

A.6 Proof of Theorem 13

Algorithm 5 is the complete version of `Check`. We refer to that in the proof.

Proof. The proof is by induction on the structure of ψ. The thesis trivially follows for the cases $\psi = r$ (regular expression), $\psi = \neg\psi'$, $\psi = \psi_1 \wedge \psi_2$, and $\psi = \langle \mathrm{B} \rangle\, \psi'$.

Let us now assume $\psi = \langle \overline{\mathrm{B}} \rangle\, \psi'$.
$\mathtt{Check}(\mathcal{K}, \psi, s, G, \mathcal{D}(\Phi)) = \top$ if and only if, for some $b'' \in \{1, \ldots, |S| \cdot (2|\psi'|+1) \cdot 2^{2 \sum_{\ell=1}^{u} |r_\ell| - 1}\}$ and some $(G'', \mathcal{D}(\Phi)'', s'') \in \mathsf{Conf}(\mathcal{K}, \psi)$ $(= \mathsf{Conf}(\mathcal{K}, \psi'))$, we have $\mathtt{Reach}(\mathcal{K}, \psi', (G, \mathcal{D}(\Phi), s), (G'', \mathcal{D}(\Phi)'', s''), b'') = \top$ and $\mathtt{Check}(\mathcal{K}, \psi', s'', G'', \mathcal{D}(\Phi)'') = \top$. We prove first the following claim.

Claim. Let $b \in \mathbb{N}$, $b > 0$. Let $\tilde{\rho} \in \mathrm{Trc}_{\mathcal{K}}$ be a trace with $\tilde{s} = \mathrm{lst}(\tilde{\rho})$. Let $\tilde{G}$ be the subset of formulas in $\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi')$ that hold on some proper prefix of $\tilde{\rho}$. Let $\tilde{\mathcal{D}}(\Phi)$ be the current configuration of states of the DFAs associated with the regular expressions in Φ, reached from the initial states after reading $\mu(\tilde{\rho}(1, |\tilde{\rho}| - 1))$.

Algorithm 5 $\texttt{Check}(\mathcal{K}, \psi, s, G, \mathcal{D}(\Phi))$

if $\psi = r$ **then** ◁ *r is a regular expression*
  if the current state of the DFA for r in $\texttt{advance}(\mathcal{D}(\Phi), \mu(s))$ is final **then**
    return $\top$
  else
    return $\bot$
else if $\psi = \neg\psi'$ **then**
  return not $\texttt{Check}(\mathcal{K}, \psi', s, G, \mathcal{D}(\Phi))$
else if $\psi = \psi_1 \wedge \psi_2$ **then**
  return $\texttt{Check}(\mathcal{K}, \psi_1, s, G \cap \mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi_1), \mathcal{D}(\Phi))$ **and** $\texttt{Check}(\mathcal{K}, \psi_2, s, G \cap \mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi_2), \mathcal{D}(\Phi))$
else if $\psi = \langle \mathrm{B} \rangle \psi'$ **then**
  if $\psi' \in G$ **then**
    return $\top$
  else
    return $\bot$
else if $\psi = \langle \overline{\mathrm{B}} \rangle \psi'$ **then**
  for each $b \in \{1, \ldots, |S| \cdot (2|\psi'| + 1) \cdot 2^{2\sum_{\ell=1}^{u} |r_\ell|} - 1\}$
    and each $(G', \mathcal{D}(\Phi)', s') \in \mathsf{Conf}(\mathcal{K}, \psi)$ **do** ◁ *$r_1, .., r_u$ are the r.e. of ψ'*
    if $\texttt{Reach}(\mathcal{K}, \psi', (G, \mathcal{D}(\Phi), s), (G', \mathcal{D}(\Phi)', s'), b)$ **and** $\texttt{Check}(\mathcal{K}, \psi', s', G', \mathcal{D}(\Phi)')$ **then**
      return $\top$
  return $\bot$

For $(\tilde{G}, \tilde{\mathcal{D}}(\Phi), \tilde{s})$, $(G', \mathcal{D}(\Phi)', s') \in \mathsf{Conf}(\mathcal{K}, \psi')$, $\texttt{Reach}(\mathcal{K}, \psi', (\tilde{G}, \tilde{\mathcal{D}}(\Phi), \tilde{s}), (G', \mathcal{D}(\Phi)', s'), b) = \top$ iff there exists $\rho' \in \mathrm{Trc}_{\mathcal{K}}$ such that $\tilde{\rho} \cdot \rho' \in \mathrm{Trc}_{\mathcal{K}}$, $|\rho'| = b$, $\mathrm{lst}(\rho') = s'$, G' is the subset of formulas in $\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi')$ that hold on some proper prefix of $\tilde{\rho} \cdot \rho'$, and $\mathcal{D}(\Phi)'$ is the current configuration of the DFAs associated with the regular expressions of Φ, after reading $\mu(\tilde{\rho} \cdot \rho'(1, |\tilde{\rho} \cdot \rho'| - 1))$.

Proof. The proof is by induction on $b \geq 1$.

If $b = 1$, $\texttt{Reach}(\mathcal{K}, \psi', (\tilde{G}, \tilde{\mathcal{D}}(\Phi), \tilde{s}), (G', \mathcal{D}(\Phi)', s'), b) = \top$ if and only if $\texttt{Compatible}(\mathcal{K}, \psi', (\tilde{G}, \tilde{\mathcal{D}}(\Phi), \tilde{s}), (G', \mathcal{D}(\Phi)', s')) = \top$. This happens if and only if:

1. $(\tilde{s}, s') \in R$—i.e., $(\tilde{s}, s')$ is an edge of $\mathcal{K}$;
2. $\texttt{advance}(\tilde{\mathcal{D}}(\Phi), \mu(\tilde{s})) = \mathcal{D}(\Phi)'$;
3. $\tilde{G} \subseteq G'$;
4. for each $\varphi \in (G' \setminus \tilde{G})$, $\texttt{Check}(\mathcal{K}, \varphi, \tilde{s}, \tilde{G} \cap \mathsf{Subf}_{\langle \mathrm{B} \rangle}(\varphi), \tilde{\mathcal{D}}(\Phi)) = \top$;
5. for each $\varphi \in (\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi') \setminus G')$, $\texttt{Check}(\mathcal{K}, \varphi, \tilde{s}, \tilde{G} \cap \mathsf{Subf}_{\langle \mathrm{B} \rangle}(\varphi), \tilde{\mathcal{D}}(\Phi)) = \bot$.

Let $\rho' = s'$. ($\Rightarrow$) By the inductive hypothesis (of the external theorem over $\tilde{\rho}$), by 4. it follows that $\mathcal{K}, \tilde{\rho} \models \varphi$ for each $\varphi \in (G' \setminus \tilde{G})$. By 5. it follows that $\mathcal{K}, \tilde{\rho} \not\models \varphi$ for each $\varphi \in (\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi') \setminus G')$. The claim follows.

Conversely, ($\Leftarrow$) 1., 2., and 3. easily follow. Moreover it must hold that $\mathcal{K}, \tilde{\rho} \models \varphi$ for each $\varphi \in (G' \setminus \tilde{G})$, and $\mathcal{K}, \tilde{\rho} \not\models \varphi$ for each $\varphi \in (\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi') \setminus G')$: 4. and 5. follow by the inductive hypothesis (of the external theorem).

If $b \geq 2$, $\texttt{Reach}(\mathcal{K}, \psi', (\tilde{G}, \tilde{\mathcal{D}}(\Phi), \tilde{s}), (G', \mathcal{D}(\Phi)', s'), b) = \top$ if and only if, for some $(G_3, \mathcal{D}(\Phi)_3, s_3) \in \mathsf{Conf}(\mathcal{K}, \psi')$, $\texttt{Reach}(\mathcal{K}, \psi', (\tilde{G}, \tilde{\mathcal{D}}(\Phi), \tilde{s}), (G_3, \mathcal{D}(\Phi)_3, s_3), \lfloor b/2 \rfloor) = \top$ and $\texttt{Reach}(\mathcal{K}, \psi', (G_3, \mathcal{D}(\Phi)_3, s_3), (G', \mathcal{D}(\Phi)', s'), b - \lfloor b/2 \rfloor) = \top$.

($\Rightarrow$) By the inductive hypothesis (over b), there exists $\rho_3 \in \mathrm{Trc}_{\mathcal{K}}$ such that $\tilde{\rho} \cdot \rho_3 \in \mathrm{Trc}_{\mathcal{K}}$, $|\rho_3| = \lfloor b/2 \rfloor$, $\mathrm{lst}(\rho_3) = s_3$, G_3 is the subset of subformulas in $\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi')$ that hold on some proper prefix of $\tilde{\rho} \cdot \rho_3$, and $\mathcal{D}(\Phi)_3$ is the current configuration of the DFAs associated with the regular expressions in Φ, after reading $\mu(\tilde{\rho} \cdot \rho_3(1, |\tilde{\rho} \cdot \rho_3| - 1))$.

By the inductive hypothesis (over b, applied to the trace $\tilde{\rho} \cdot \rho_3$), there exists $\rho' \in \mathrm{Trc}_{\mathcal{K}}$ such that $\tilde{\rho} \cdot \rho_3 \cdot \rho' \in \mathrm{Trc}_{\mathcal{K}}$, $|\rho'| = b - \lfloor b/2 \rfloor$, $\mathrm{lst}(\rho') = s'$, G' is the subset of subformulas in $\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi')$ that hold on some proper prefix of $\tilde{\rho} \cdot \rho_3 \cdot \rho'$, and $\mathcal{D}(\Phi)'$ is the current configuration of the DFAs associated with the regular expressions in Φ, after reading $\mu(\tilde{\rho} \cdot \rho_3 \cdot \rho'(1, |\tilde{\rho} \cdot \rho_3 \cdot \rho'| - 1))$. The claim follows, as $\rho_3 \cdot \rho' \in \mathrm{Trc}_{\mathcal{K}}$ and $|\rho_3 \cdot \rho'| = b$.

($\Leftarrow$) Conversely, there exists $\rho' \in \mathrm{Trc}_{\mathcal{K}}$ such that $\tilde{\rho} \cdot \rho' \in \mathrm{Trc}_{\mathcal{K}}$, $|\rho'| = b \geq 2$, $\mathrm{lst}(\rho') = s'$, G' is the subset of subformulas in $\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi')$ that hold on some proper prefix of $\tilde{\rho} \cdot \rho'$, and $\mathcal{D}(\Phi)'$ is the current configuration of the DFAs associated with the regular expressions in Φ, after reading $\mu(\tilde{\rho} \cdot \rho'(1, |\tilde{\rho} \cdot \rho'| - 1))$. Let us split $\rho' = \rho_3 \cdot \rho_4$, where $|\rho_3| = \lfloor b/2 \rfloor$ and $|\rho_4| = b - \lfloor b/2 \rfloor$. Let $(G_3, \mathcal{D}(\Phi)_3, s_3) \in \mathsf{Conf}(\mathcal{K}, \psi')$ be such that $\mathcal{D}(\Phi)_3$ is the current configuration of the DFAs associated with the regular expressions in Φ, after reading $\mu(\tilde{\rho} \cdot \rho_3(1, |\tilde{\rho} \cdot \rho_3| - 1))$, $s_3 = \mathrm{lst}(\rho_3)$, G_3 is the subset of subformulas in $\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi')$ that hold on some proper prefix of $\tilde{\rho} \cdot \rho_3$. By the inductive hypothesis (on b over $\tilde{\rho} \cdot \rho_3$), $\mathtt{Reach}(\mathcal{K}, \psi', (G_3, \mathcal{D}(\Phi)_3, s_3), (G', \mathcal{D}(\Phi)', s'), b - \lfloor b/2 \rfloor) = \top$. Moreover, by the inductive hypothesis (on b over $\tilde{\rho}$), $\mathtt{Reach}(\mathcal{K}, \psi', (\tilde{G}, \tilde{\mathcal{D}}(\Phi), \tilde{s}), (G_3, \mathcal{D}(\Phi)_3, s_3), \lfloor b/2 \rfloor) = \top$.

Hence both the recursive calls at line 6 return $\top$, when at line 5 $(G_3, \mathcal{D}(\Phi)_3, s_3)$ is considered by the loop. Thus $\mathtt{Reach}(\mathcal{K}, \psi', (\tilde{G}, \tilde{\mathcal{D}}(\Phi), \tilde{s}), (G', \mathcal{D}(\Phi)', s'), b)$ returns $\top$.

This concludes the proof of the claim. □

($\Rightarrow$) Let us now assume that in `Check`, at lines 15–19, for some $b'' \in \{1, \ldots, |S| \cdot (2|\psi'|+1) \cdot 2^{2 \sum_{\ell=1}^{u} |r_\ell|} - 1\}$ and some $(G'', \mathcal{D}(\Phi)'', s'') \in \mathsf{Conf}(\mathcal{K}, \psi)$ $(= \mathsf{Conf}(\mathcal{K}, \psi'))$, we have $\mathtt{Reach}(\mathcal{K}, \psi', (G, \mathcal{D}(\Phi), s), (G'', \mathcal{D}(\Phi)'', s''), b'') = \top$ and $\mathtt{Check}(\mathcal{K}, \psi', s'', G'', \mathcal{D}(\Phi)'') = \top$. By the previous claim, there exists $\rho'' \in \mathrm{Trc}_{\mathcal{K}}$ such that $\rho \cdot \rho'' \in \mathrm{Trc}_{\mathcal{K}}$, $\mathrm{lst}(\rho'') = s''$, G'' is the subset of subformulas in $\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi')$ that hold on some proper prefix of $\rho \cdot \rho''$, and $\mathcal{D}(\Phi)''$ is the current configuration of the DFAs associated with the regular expressions of Φ, after reading $\mu(\rho \cdot \rho''(1, |\rho \cdot \rho''| - 1))$. By the inductive hypothesis, since $\mathtt{Check}(\mathcal{K}, \psi', s'', G'', \mathcal{D}(\Phi)'') = \top$, we have $\mathcal{K}, \rho \cdot \rho'' \models \psi'$. Thus $\mathcal{K}, \rho \models \langle \overline{\mathrm{B}} \rangle \psi'$.

($\Leftarrow$) Conversely, if $\mathcal{K}, \rho \models \langle \overline{\mathrm{B}} \rangle \psi'$, we have $\mathcal{K}, \rho \cdot \rho'' \models \psi'$ for some $\rho'' \in \mathrm{Trc}_{\mathcal{K}}$, with $\rho \cdot \rho'' \in \mathrm{Trc}_{\mathcal{K}}$. By the exponential small-model Theorem 12, there exists $\rho' \in \mathrm{Trc}_{\mathcal{K}}$ such that $\mathrm{lst}(\rho'') = \mathrm{lst}(\rho')$, $|\rho'| \leq |S| \cdot (2|\psi'| + 1) \cdot 2^{2 \sum_{\ell=1}^{u} |r_\ell|} - 1$ (the factor 2 in front of $|\psi'|$ is due to the fact that the exponential small-model property requires a formula in NNF), $\rho \cdot \rho' \in \mathrm{Trc}_{\mathcal{K}}$ and $\mathcal{K}, \rho \cdot \rho' \models \psi'$. Let G' be the subset of subformulas in $\mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi') = \mathsf{Subf}_{\langle \mathrm{B} \rangle}(\psi)$ that hold on some proper prefix of $\rho \cdot \rho'$, and $\mathcal{D}(\Phi)'$ be the current configuration of the DFAs associated with the regular expressions in Φ, after reading $\mu(\rho \cdot \rho'(1, |\rho \cdot \rho'| - 1))$. By the inductive hypothesis (over $\rho \cdot \rho'$), $\mathtt{Check}(\mathcal{K}, \psi', \mathrm{lst}(\rho'), G', \mathcal{D}(\Phi)') = \top$.

By the previous claim, $\texttt{Reach}(\mathcal{K}, \psi', (G, \mathcal{D}(\Phi), s), (G', \mathcal{D}(\Phi)', \mathrm{lst}(\rho')), |\rho'|) = \top$, hence $\texttt{Check}(\mathcal{K}, \psi, s, G, \mathcal{D}(\Phi)) = \top$.

This concludes the proof of the theorem. □

A.7 Proof of Theorem 14

Proof. If $\mathcal{K} \models \Phi$, then for all $\rho \in \mathrm{Trc}_{\mathcal{K}}$ with $\mathrm{fst}(\rho) = s_0$, we have $\mathcal{K}, \rho \models \Phi$, hence $\mathcal{K}, s_0 \models \Phi$, and $\mathcal{K}, s_0 \cdot \rho' \models \Phi$ for all $s_0 \cdot \rho' \in \mathrm{Trc}_{\mathcal{K}}$, thus $\mathcal{K}, s_0 \models [\overline{B}]\Phi$, namely, $\mathcal{K}, s_0 \not\models \langle \overline{\mathrm{B}} \rangle \neg\Phi$. By Theorem 13, $\texttt{Check}(\mathcal{K}, \neg\Phi, s_0, \emptyset, \mathcal{D}(\Phi)_0) = \bot$ and $\texttt{Check}(\mathcal{K}, \langle \overline{\mathrm{B}} \rangle \neg\Phi, s_0, \emptyset, \mathcal{D}(\Phi)_0) = \bot$ implying that $\texttt{CheckAux}(\mathcal{K}, \Phi)$ returns $\top$.

Conversely, if the procedure $\texttt{CheckAux}(\mathcal{K}, \Phi)$ returns $\top$, then it must be $\texttt{Check}(\mathcal{K}, \neg\Phi, s_0, \emptyset, \mathcal{D}(\Phi)_0) = \bot$ and $\texttt{Check}(\mathcal{K}, \langle \overline{\mathrm{B}} \rangle \neg\Phi, s_0, \emptyset, \mathcal{D}(\Phi)_0) = \bot$. By Theorem 13 applied to the trace $\rho = s_0$, we have $\mathcal{K}, s_0 \not\models \neg\Phi$ and $\mathcal{K}, s_0 \not\models \langle \overline{\mathrm{B}} \rangle \neg\Phi$, and, therefore, $\mathcal{K} \models \Phi$. □

A.8 MC for $\mathsf{A\overline{A}B\overline{B}}$ is PSPACE-complete (in detail)

We show that the algorithm `CheckAux` can be used as a basic engine to design a **PSPACE** MC algorithm for $\mathsf{A\overline{A}B\overline{B}}$. The idea is that, being the proposition letters related with regular expressions, the modalities $\langle \mathrm{A} \rangle$ and $\langle \overline{\mathrm{A}} \rangle$ do not augment the expressiveness of the fragment $\mathsf{B\overline{B}}$. In particular, we shall show how $\langle \mathrm{A} \rangle$ and $\langle \overline{\mathrm{A}} \rangle$, occurring in an $\mathsf{A\overline{A}B\overline{B}}$ formula, can suitably be "absorbed" and replaced by fresh proposition letters.

By definition, $\mathcal{K}, \rho \models \langle \mathrm{A} \rangle \psi$ if and only if there exists a trace $\tilde{\rho} \in \mathrm{Trc}_{\mathcal{K}}$ such that $\mathrm{lst}(\rho) = \mathrm{fst}(\tilde{\rho})$ and $\mathcal{K}, \tilde{\rho} \models \psi$. An immediate consequence is that, for any $\rho' \in \mathrm{Trc}_{\mathcal{K}}$ with $\mathrm{lst}(\rho) = \mathrm{lst}(\rho')$, $\mathcal{K}, \rho \models \langle \mathrm{A} \rangle \psi \iff \mathcal{K}, \rho' \models \langle \mathrm{A} \rangle \psi$. Analogous considerations can be done for the symmetrical modality $\langle \overline{\mathrm{A}} \rangle$ with respect to initial states of traces. In general, if two traces have the same final state (resp., first state), either both of them satisfy a formula $\langle \mathrm{A} \rangle \psi$ (resp., $\langle \mathrm{A} \rangle \psi$), or none of them does. Therefore, for a formula $\langle \mathrm{A} \rangle \psi$ (resp., $\langle \overline{\mathrm{A}} \rangle \psi$), we can determine the subset $S_{\langle \mathrm{A} \rangle \psi}$ (resp., $S_{\langle \overline{\mathrm{A}} \rangle \psi}$) of the set of states S of the Kripke structure such that, for any $\rho \in \mathrm{Trc}_{\mathcal{K}}$, $\mathcal{K}, \rho \models \langle \mathrm{A} \rangle \psi$ (resp., $\mathcal{K}, \rho \models \langle \overline{\mathrm{A}} \rangle \psi$) if and only if $\mathrm{lst}(\rho) \in S_{\langle \mathrm{A} \rangle \psi}$ (resp., $\mathrm{fst}(\rho) \in S_{\langle \overline{\mathrm{A}} \rangle \psi}$).

The idea is that we can identify each state $s \in S$ exploiting a set of fresh proposition letters $\{q_s \mid s \in S\}$; then we define, for a subformula $\langle \mathrm{A} \rangle \psi$ (resp., $\langle \overline{\mathrm{A}} \rangle \psi$), a regular expression $r_{\langle \mathrm{A} \rangle \psi}$ (resp., $r_{\langle \overline{\mathrm{A}} \rangle \psi}$) characterizing the set of traces which model the subformula, and finally we replace any occurrence of $\langle \mathrm{A} \rangle \psi$ (resp., $\langle \overline{\mathrm{A}} \rangle \psi$) by a fresh interval property associated with this regular expression. More formally, instead of $\mathcal{K} = (\mathcal{AP}, S, R, \mu, s_0)$, we consider $\mathcal{K}' = (\mathcal{AP}', S, R, \mu', s_0)$, with $\mathcal{AP}' := \mathcal{AP} \cup \{q_s \mid s \in S\}$ and $\mu'(s) = \{q_s\} \cup \mu(s)$ for any $s \in S$. For the formulas $\langle \mathrm{A} \rangle \psi$ and $\langle \overline{\mathrm{A}} \rangle \psi$, the regular expressions $r_{\langle \mathrm{A} \rangle \psi}$ and $r_{\langle \overline{\mathrm{A}} \rangle \psi}$ are: $r_{\langle \mathrm{A} \rangle \psi} := \top^* \cdot \left(\bigcup_{s \in S_{\langle \mathrm{A} \rangle \psi}} q_s \right)$ and $r_{\langle \overline{\mathrm{A}} \rangle \psi} := \left(\bigcup_{s \in S_{\langle \overline{\mathrm{A}} \rangle \psi}} q_s \right) \cdot \top^*$. By definition $\mathcal{K}, \rho \models r_{\langle \mathrm{A} \rangle \psi}$ iff $\mathrm{lst}(\rho) \in S_{\langle \mathrm{A} \rangle \psi}$ iff $\mathcal{K}, \rho \models \langle \mathrm{A} \rangle \psi$.

We can now sketch the procedure for "reducing" the MC problem for $\mathsf{A\overline{A}B\overline{B}}$ to the MC problem for $\mathsf{B\overline{B}}$. The idea is to iteratively rewrite a formula Φ of $\mathsf{A\overline{A}B\overline{B}}$

until it gets converted to an (equivalent) formula of $\mathsf{B\overline{B}}$. At each step, we select an occurrence of a subformula of Φ, either of the form $\langle \mathrm{A} \rangle \psi$ or $\langle \overline{\mathrm{A}} \rangle \psi$, devoid of any internal occurrences of modalities $\langle \mathrm{A} \rangle$ and $\langle \overline{\mathrm{A}} \rangle$. For such an occurrence, say $\langle \mathrm{A} \rangle \psi$, we have to compute the set $S_{\langle \mathrm{A} \rangle \psi}$. For this purpose we can run a variant `CheckAux'`$(\mathcal{K}, \Psi, s)$ of the MC procedure `CheckAux`$(\mathcal{K}, \Psi)$, which invokes `Check` at line 2 on the additional parameter (state) s, instead of s_0. For each $s \in S$, we invoke `CheckAux'`$(\mathcal{K}, \neg\psi, s)$, deciding that $s \in S_{\langle \mathrm{A} \rangle \psi}$ iff the procedure returns $\bot$. Then we replace $\langle \mathrm{A} \rangle \psi$ in Φ with a fresh interval property proposition letter associated with the regular expression $r_{\langle \mathrm{A} \rangle \psi}$, obtaining a formula Φ'. To deal with subformulas of the form $\langle \overline{\mathrm{A}} \rangle \psi$, we have to introduce a slight variant of the procedure `Check`, which finds traces leading to (and not starting from) a given state. Now, if the resulting formula Φ' is in $\mathsf{B\overline{B}}$, we have finished the conversion. Otherwise we can proceed with another iteration of the conversion step over Φ'.

Considering that the sets $S_{\langle \mathrm{A} \rangle \psi}$, $S_{\langle \overline{\mathrm{A}} \rangle \psi'}$ and the regular expressions $r_{\langle \mathrm{A} \rangle \psi}$ and $r_{\langle \overline{\mathrm{A}} \rangle \psi}$ have a size linear in $|S|$, we can conclude with the following theorem.

Theorem 18. *The MC problem for* $\mathsf{A\overline{A}B\overline{B}}$ *formulas over finite Kripke structures is in* **PSPACE**.

By symmetry we can show that MC for $\mathsf{A\overline{A}E\overline{E}}$ formulas is also a **PSPACE** problem.

The **PSPACE**-hardness of MC for $\mathsf{B\overline{B}}$ and $\mathsf{A\overline{A}B\overline{B}}$ directly follows from that of the smallest fragment Prop (the purely propositional fragment of HS) which is stated by Theorem 19. As a matter of fact, we prove that Prop is hard for **PSPACE** by a reduction from the **PSPACE**-complete *universality problem for regular expressions* (the problem of deciding, for a regular expression r with $\mathcal{L}(r) \subseteq \Sigma^*$ and $|\Sigma| \geq 2$, whether $\mathcal{L}(r) = \Sigma^*$).

Theorem 19. *The MC problem for formulas of* Prop *over finite Kripke structures is* **PSPACE**-*hard (under* **LOGSPACE** *reductions).*

Proof. Given a regular expression r with $\mathcal{L}(r) \subseteq \Sigma^*$, let us define $\mathcal{K} = (\Sigma, \{s_0\} \cup \Sigma, R, \mu, s_0)$, where $s_0 \notin \Sigma$, $\mu(s_0) = \emptyset$, for $c \in \Sigma$ we have $\mu(c) = \{c\}$, and $R = \{(s_0, c) \mid c \in \Sigma\} \cup \{(c, c') \mid c, c' \in \Sigma\}$. It holds that

$$\mathcal{L}(r) = \Sigma^* \iff \mathcal{K} \models \top \cdot \overline{r},$$

where $\overline{r}$ is a RE over Σ, *syntactically* the same as r. Note that whereas r is a standard regular expression—defining a finitary language over Σ—$\overline{r}$, even though syntactically the same as r, defines a finitary language *over* 2^Σ, as pointed out in Section 2. The distinction between r and $\overline{r}$ is kept in the rest of the proof in order to avoid confusion between the two "roles" of r.

We show by induction on the structure of r that, for all $w \in \Sigma^*$, $w \in \mathcal{L}(r) \iff \mathcal{K}, w \models \overline{r}$. The thesis follows as $\mathcal{K}, w \models \overline{r}$ if and only if $\mathcal{K}, s_0 \cdot w \models \top \cdot \overline{r}$.

- $r = \varepsilon$. Then, $w \in \mathcal{L}(\varepsilon)$ iff $w = \varepsilon$ iff $\mu(w) \in \mathcal{L}(\overline{\varepsilon}) = \{\varepsilon\}$ iff $\mathcal{K}, w \models \overline{\varepsilon}$.
- $r = c \in \Sigma$. Then, we have $w \in \mathcal{L}(c)$ iff $w = c$, thus $\mu(w) = \{c\} \in \mathcal{L}(\overline{c})$, and $\mathcal{K}, w \models \overline{c}$. Conversely, if $\mathcal{K}, w \models \overline{c}$ we have $\mu(w) \in \mathcal{L}(\overline{c}) = \{A \in 2^\Sigma \mid c \in A\}$. In particular $|w| = 1$. Moreover, by definition of μ, $\mu(w)$ is a singleton, hence $\mu(w) = \{c\}$. By definition of $\mathcal{K}$, $w = c$, thus $w \in \mathcal{L}(c)$.

- $r = r_1 \cdot r_2$. $w \in \mathcal{L}(r_1 \cdot r_2)$ iff $w = w_1 \cdot w_2$ and $w_1 \in \mathcal{L}(r_1)$ and $w_2 \in \mathcal{L}(r_2)$. By applying the inductive hypothesis, $\mathcal{K}, w_1 \models \overline{r_1}$ and $\mathcal{K}, w_2 \models \overline{r_2}$, thus $\mu(w_1) \in \mathcal{L}(\overline{r_1})$ and $\mu(w_2) \in \mathcal{L}(\overline{r_2})$. It follows that $\mu(w) = \mu(w_1) \cdot \mu(w_2) \in \mathcal{L}(\overline{r_1}) \cdot \mathcal{L}(\overline{r_2}) = \mathcal{L}(\overline{r_1 \cdot r_2})$, namely $\mathcal{K}, w \models \overline{r_1 \cdot r_2}$. Conversely, $\mu(w) \in \mathcal{L}(\overline{r_1 \cdot r_2}) = \mathcal{L}(\overline{r_1}) \cdot \mathcal{L}(\overline{r_2})$. Hence $\mu(w_1) \in \mathcal{L}(\overline{r_1})$ and $\mu(w_2) \in \mathcal{L}(\overline{r_2})$, for some $w_1 \cdot w_2 = w$. By the inductive hypothesis, $w_1 \in \mathcal{L}(r_1)$ and $w_2 \in \mathcal{L}(r_2)$, hence $w \in \mathcal{L}(r_1 \cdot r_2)$.
- $r = r_1 \cup r_2$. $w \in \mathcal{L}(r_1 \cup r_2)$ iff $w \in \mathcal{L}(r_i)$ for some $i = 1, 2$. By the inductive hypothesis this is true iff $\mathcal{K}, w \models \overline{r_i}$, iff $\mu(w) \in \mathcal{L}(\overline{r_i})$, iff $\mu(w) \in \mathcal{L}(\overline{r_1 \cup r_2})$, iff $\mathcal{K}, w \models \overline{r_1 \cup r_2}$.
- $r = r_1^*$. The thesis trivially holds if $w = \varepsilon$. Let us now assume $w \neq \varepsilon$. $w \in \mathcal{L}(r_1^*)$ iff $w = w_1 \cdots w_t$, $t \geq 1$, such that $w_\ell \in \mathcal{L}(r_1)$ for all $1 \leq \ell \leq t$. By the inductive hypothesis, $\mathcal{K}, w_\ell \models \overline{r_1}$, thus $\mu(w_\ell) \in \mathcal{L}(\overline{r_1})$, and $\mu(w) \in \mathcal{L}(\overline{r_1^*})$. We conclude that $\mathcal{K}, w \models \overline{r_1^*}$. Conversely, $\mu(w) \in \mathcal{L}(\overline{r_1^*}) = (\mathcal{L}(\overline{r_1}))^*$, hence it must be the case that $w = w_1 \cdots w_t$, $t \geq 1$, such that $\mu(w_\ell) \in \mathcal{L}(\overline{r_1})$. By the inductive hypothesis, $w_\ell \in \mathcal{L}(r_1)$, hence $w \in \mathcal{L}(r_1^*)$.

  Finally, we can build $\mathcal{K}$ using logarithmic working space. □

By Theorems 18 and 19, it immediately follows that MC for any (proper or improper) sub-fragment of $\mathsf{A\overline{A}B\overline{B}}$ (and $\mathsf{A\overline{A}E\overline{E}}$) is **PSPACE**-complete (Theorem 16).