University of Udine

Department of Mathematics and Computer Science

PREPRINT

Satisfiability and Model Checking for the Logic of Sub-Intervals under the Homogeneity Assumption

Laura Bozzelli, Alberto Molinari, Angelo Montanari, Adriano Peron, Pietro Sala

Preprint nr.: 4/2017

Reports available from: https://www.dimi.uniud.it/preprints/

Satisfiability and Model Checking for the Logic of Sub-Intervals under the Homogeneity Assumption

Laura Bozzelli, Alberto Molinari, Angelo Montanari,
Adriano Peron, and Pietro Sala

Abstract

In this paper, we investigate the finite satisfiability and model checking problems for the logic D of the sub-interval relation under the homogeneity assumption, that constrains a proposition letter to hold over an interval if and only if it holds over all its points. First we prove that the satisfiability problem for D, over finite linear orders, is **PSPACE**-complete; then we show that its model checking problem, over finite Kripke structures, is **PSPACE**-complete as well.

1 Introduction

For a long time, interval temporal logic (ITL) was considered as an attractive, but impractical, alternative to standard point-based ones. On the one hand, as pointed out, among others, by Kamp and Reyle [KR93], "truth, as it pertains to language in the way we use it, relates sentences not to instants but to temporal intervals", and thus ITL is a natural choice for a specification/representation language; on the other hand, the high undecidability of the satisfiability problem for the most well-known ITLs, such as Halpern and Shoham's HS [HS91] and Venema's CDT [Ven91], prevented an extensive use of them (in fact, some very restricted variants of them have been successfully applied in formal verification and AI over the years).

The recent discovery of a significant number of expressive enough and computationally well-behaved ITLs changed the landscape a lot [DGMS11, Mon16]. Among them, the logic A$\overline{\text{A}}$ of temporal neighborhood [BGMS09] and the logic D of (temporal) sub-intervals [BGMS10] have a central position. In this paper, we focus on the latter one. D features one modality only, which corresponds to the Allen relation *during* [All83]. Since any sub-interval can be defined as an initial sub-interval of an ending one, or, equivalently, as an ending sub-interval of an initial one, it is a (proper) fragment of the logic BE of Allen's relations *started-by* and *finished-by*. From a computational point of view, D is a real character: its satisfiability problem is **PSPACE**-complete over the class of dense linear orders [BGMS10, Sha04] (the problem is undecidable for BE [Lod00]), it becomes undecidable when the logic is interpreted over the classes of finite and discrete linear orders [MM14], and it is still unknown over the class of all linear orders. As for its expressiveness, unlike A$\overline{\text{A}}$—which is expressively complete with respect to the two-variable fragment of first-order logic for binary relational structures over various linearly-ordered domains [BGMS09, Ott01]—three variables are needed to encode D in first-order logic (the two-variable property is a sufficient condition for decidability, but it is not a necessary one).

In this paper, we show that the decidability of the satisfiability problem for D over the class of finite linear orders can be recovered under the homogeneity assumption (such an assumption constrains a proposition letter to hold over an interval if and only if it holds over all its points). We first prove that the problem belongs to **PSPACE** by exploiting a suitable contraction method.

In addition, we prove that the proposed satisfiability checking algorithm can be turned into a **PSPACE** model checking procedure for D formulas over finite Kripke structures (under the homogeneity assumption); **PSPACE**-hardness of both problems follows via a reduction from the language universality problem of nondeterministic finite-state automata. **PSPACE**-completeness of D model checking strongly contrasts with the case of BE, for which only a nonelementary model checking procedure is known [MMM$^+$16] and an **EXPSPACE**-hardness result has been given [BMM$^+$16].

The rest of the paper is organized as follows. In Section 2, we provide some background knowledge. Then, in Section 3, we prove the **PSPACE** membership of the satisfiability problem for D over finite linear orders (under the homogeneity assumption). Finally, in Section 4, we show that the model checking problem for D over finite Kripke structures (again, under the homogeneity assumption) is in **PSPACE** as well.

2 The logic D of the sub-interval relation

Let $\mathbb{S} = \langle S, < \rangle$ be a linear order. An *interval* over $\mathbb{S}$ is an ordered pair $[x, y]$, where $x \leq y$. We denote the set of all intervals over $\mathbb{S}$ by $\mathbb{I}(\mathbb{S})$. We consider three possible *sub-interval relations*: (*i*) the *reflexive* sub-interval relation (denoted as $\sqsubseteq$), defined by $[x, y] \sqsubseteq [x', y']$ iff $x' \leq x$ and $y \leq y'$, (*ii*) the *proper (or irreflexive)* sub-interval relation (denoted as $\sqsubset$), defined by $[x, y] \sqsubset [x', y']$ iff $[x, y] \sqsubseteq [x', y']$ and $[x, y] \neq [x', y']$, and (*iii*) the *strict* sub-interval relation (denoted as $\Subset$), defined by $[x, y] \Subset [x', y']$ iff $x' < x$ and $y < y'$.

The three modal logics $\mathrm{D}_{\sqsubseteq}$, $\mathrm{D}_{\sqsubset}$, and $\mathrm{D}_{\Subset}$ feature the same language, consisting of a set $\mathcal{AP}$ of proposition letters/variables, the logical connectives $\neg$ and $\vee$, and the modal operator $\langle D \rangle$. Formally, formulae are defined by the grammar: $\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid \langle D \rangle \varphi$, with $p \in \mathcal{AP}$. The other connectives, as well as the logical constants $\top$ (true) and $\bot$ (false), are defined as usual; moreover, the dual universal modal operator $[D]\varphi$ is defined as $\neg\langle D \rangle \neg\varphi$. The length of a formula φ, denoted as $|\varphi|$, is the number of sub-formulas of φ.

The semantics of $\mathrm{D}_{\Subset}$, $\mathrm{D}_{\sqsubset}$, and $\mathrm{D}_{\sqsubseteq}$ only differ in the interpretation of the $\langle D \rangle$ operator. For the sake of brevity, we use $\circ \in \{\Subset, \sqsubset, \sqsubseteq\}$ as a shorthand for any of the three sub-interval relations. The semantics of a sub-interval logic $\mathrm{D}_\circ$ is defined in terms of *interval models* $\mathbf{M} = \langle \mathbb{I}(\mathbb{S}), \circ, \mathcal{V} \rangle$. The *valuation function* $\mathcal{V} : \mathcal{AP} \mapsto 2^{\mathbb{I}(\mathbb{S})}$ assigns to every proposition variable p the set of intervals $\mathcal{V}(p)$ over which p holds. The *satisfiability relation* $\models$ is defined as:

- for every proposition letter $p \in \mathcal{AP}$, $\mathbf{M}, [x, y] \models p$ iff $[x, y] \in \mathcal{V}(p)$;
- $\mathbf{M}, [x, y] \models \neg\psi$ iff $\mathbf{M}, [x, y] \not\models \psi$ (i.e., it is not true that $\mathbf{M}, [x, y] \models \psi$);
- $\mathbf{M}, [x, y] \models \psi_1 \vee \psi_2$ iff $\mathbf{M}, [x, y] \models \psi_1$ or $\mathbf{M}, [x, y] \models \psi_2$;
- $\mathbf{M}, [x, y] \models \langle D \rangle \psi$ iff there is an interval $[x', y'] \in \mathbb{I}(\mathbb{S})$ s.t. $[x', y'] \circ [x, y]$ and $\mathbf{M}, [x', y'] \models \psi$.

A $\mathrm{D}_\circ$-formula is $\mathrm{D}_\circ$-*satisfiable* if it holds over some interval of an interval model and it is $\mathrm{D}_\circ$-*valid* if it holds over every interval of every interval model.

In this paper, we restrict our attention to the finite satisfiability problem, that is, satisfiability over the class of finite linear orders. The problem has been shown to be *undecidable* for $\mathrm{D}_{\sqsubset}$ and $\mathrm{D}_{\Subset}$ [MM14] and *decidable* for $\mathrm{D}_{\sqsubseteq}$ [MPS10]. In the following, we show that decidability can be recovered for $\mathrm{D}_{\sqsubset}$ and $\mathrm{D}_{\Subset}$ by restricting to the class of *homogeneous* interval models. We fully work out the case of $\mathrm{D}_{\sqsubset}$ (for the sake of simplicity, we will write D for $\mathrm{D}_{\sqsubset}$), and then we briefly explain how to adapt the proofs to $\mathrm{D}_{\Subset}$.

Definition 1. *A model* $\mathbf{M} = \langle \mathbb{I}(\mathbb{S}), \circ, \mathcal{V} \rangle$ *is homogeneous if, for every interval* $[x, y] \in \mathbb{I}(\mathbb{S})$ *and every* $p \in \mathcal{AP}$*, it holds that* $[x, y] \in \mathcal{V}(p)$ *iff* $[x', x'] \in \mathcal{V}(p)$ *for every* $x \leq x' \leq y$*.*

Hereafter, we will refer to the logic D interpreted over homogeneous models as $\mathrm{D}|_{\mathcal{H}om}$.

2.1 A spatial representation of interval models

We now introduce some basic definitions and notation which will be extensively used in the following. Given a D-formula φ, we define the *closure of* φ, denoted by $\mathrm{CL}(\varphi)$, as the set of all sub-formulas ψ of φ and of their negations $\neg\psi$ (we identify $\neg\neg\psi$ with ψ).

Definition 2. *Given a* D*-formula* φ*, a* φ*-atom* A *is a subset of* $\mathrm{CL}(\varphi)$ *such that:* (i) *for every* $\psi \in \mathrm{CL}(\varphi)$*,* $\psi \in A$ *iff* $\neg\psi \notin A$*, and* (ii) *for every* $\psi_1 \vee \psi_2 \in \mathrm{CL}(\varphi)$*,* $\psi_1 \vee \psi_2 \in A$ *iff* $\psi_1 \in A$ *or* $\psi_2 \in A$*.*

The idea underlying atoms is to enforce a "local" (or Boolean) form of consistency among the formulas it contains, that is, a φ-atom A is a *maximal, locally consistent subset* of $\mathrm{CL}(\varphi)$. As an example, $\neg(\psi_1 \vee \psi_2) \in A$ iff $\neg\psi_1 \in A$ and $\neg\psi_2 \in A$. However, note that the definition does not set any constraint on $\langle D \rangle \psi$ formulas, hence the word "local". We denote the set of all φ-atoms as $\mathcal{A}_\varphi$; its cardinality is clearly bounded by $2^{|\varphi|}$ (by point (i) of Definition 2). Atoms are connected by the following binary relation D_φ.

Definition 3. *Let* D_φ *be a binary relation over* $\mathcal{A}_\varphi$ *such that, for each pair of atoms* $A, A' \in \mathcal{A}_\varphi$*,* $A \; D_\varphi \; A'$ *holds iff both* $\psi \in A'$ *and* $[D]\psi \in A'$ *for each formula* $[D]\psi \in A$*.*

Let A be a φ-atom. We denote by $\mathcal{R}eq_D(A)$ the set $\{\psi \in \mathrm{CL}(\varphi) : \langle D \rangle \psi \in A\}$ of "temporal requests" of A. In particular, if $\psi \notin \mathcal{R}eq_D(A)$, then $[D]\neg\psi \in A$ (by the definition of φ-atom). Moreover, we denote by REQ_φ the set of all arguments of $\langle D \rangle$-formulas in $\mathrm{CL}(\varphi)$, namely, $\mathrm{REQ}_\varphi = \{\psi : \langle D \rangle \psi \in \mathrm{CL}(\varphi)\}$. Finally, we denote by $\mathcal{O}bs_D(A)$ the set $\{\psi \in A : \psi \in \mathrm{REQ}_\varphi\}$ of observables of A. It is easy to prove by induction the next proposition, stating that, once the proposition letters of A and its temporal requests have been fixed, A gets unambiguously determined.

Proposition 4. *For any* D*-formula* φ*, given a set* $R \subseteq \mathrm{REQ}_\varphi$ *and a set* $P \subseteq \mathrm{CL}(\varphi) \cap \mathcal{AP}$*, there exists a unique* φ*-atom* A *that satisfies* $\mathcal{R}eq_D(A) = R$ *and* $A \cap \mathcal{AP} = P$*.*

We now provide a natural interpretation of D over grid-like structures, called *compass structures*, by exploiting the existence of a natural bijection between intervals $[x, y]$ and points (x, y), with $x \leq y$, of an $S \times S$ grid, where $\mathbb{S} = \langle S, < \rangle$ is a finite linear order. Such an interpretation was originally proposed by Venema in [Ven90], and it can also be given for HS and all its (other) fragments.

As an example, Figure 1 shows four intervals $[x_0, y_0], \ldots, [x_3, y_3]$, respectively represented by the points in the grid $(x_0, y_0), \ldots, (x_3, y_3)$, such that: (i) $[x_0, y_0], [x_1, y_1], [x_2, y_2] \sqsubset [x_3, y_3]$, (ii) $[x_1, y_1] \sqsubsetneq [x_3, y_3]$, and (iii) $[x_0, y_0], [x_2, y_2] \not\sqsubset [x_3, y_3]$. The red region highlighted in Figure 1 contains all and only the points (x, y) such that $[x, y] \sqsubset [x_3, y_3]$. Allen interval relation *contains* can thus be represented as a spatial relation between pairs of points. In the following, we make use of $\sqsubset$ also for relating points, i.e., given two points $(x, y), (x', y')$ of the grid, $(x', y') \sqsubset (x, y)$ iff $(x', y') \neq (x, y)$ and $x \leq x' \leq y' \leq y$. Compass structures, repeatedly exploited to establish the following complexity results, can be formally defined as follows.

Definition 5. *Given a finite linear order* $\mathbb{S} = \langle S, < \rangle$ *and a* D*-formula* φ*, a* compass φ-structure *is a pair* $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$*, where* $\mathbb{P}_\mathbb{S}$ *is the set of points of the form* (x, y)*, with* $x, y \in S$ *and* $x \leq y$*,*

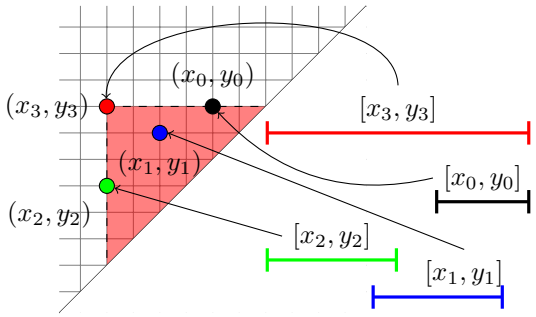

Figure 1: Correspondence between intervals and points of the compass structure.

*and $\mathcal{L}$ is a function that maps any point $(x, y) \in \mathbb{P}_\mathbb{S}$ to a φ-atom $\mathcal{L}(x, y)$ in such a way that for every pair of points $(x, y) \neq (x', y') \in \mathbb{P}_\mathbb{S}$, if $x \leq x' \leq y' \leq y$ then $\mathcal{L}(x, y)$ D_φ $\mathcal{L}(x', y')$ (*temporal consistency*).*

Due to temporal consistency, the following important property holds in compass structures.

Lemma 6. *Given a compass φ-structure $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$, for all pairs of points $(x', y'), (x, y) \in \mathbb{P}_\mathbb{S}$, if $(x', y') \sqsubset (x, y)$ then $\mathcal{R}eq_D(\mathcal{L}(x', y')) \subseteq \mathcal{R}eq_D(\mathcal{L}(x, y))$ and $\mathcal{O}bs_D(\mathcal{L}(x', y')) \subseteq \mathcal{R}eq_D(\mathcal{L}(x, y))$.*

Proof. By Definition 5 we have $\mathcal{L}(x, y)$ D_φ $\mathcal{L}(x', y')$. Let us assume by contradiction that there exists $\psi \in \mathcal{R}eq_D(\mathcal{L}(x', y')) \setminus \mathcal{R}eq_D(\mathcal{L}(x, y))$. By definition of $\mathcal{R}eq_D$ and by Definition 2, we have that $\psi \in \mathcal{R}eq_D(\mathcal{L}(x', y'))$ implies $\langle D\rangle\psi \in \mathcal{L}(x', y')$, and $\psi \notin \mathcal{R}eq_D(\mathcal{L}(x, y))$ implies $\neg\langle D\rangle\psi = [D]\neg\psi \in \mathcal{L}(x, y)$. Since $\mathcal{L}(x, y)$ D_φ $\mathcal{L}(x', y')$, then $[D]\neg\psi \in \mathcal{L}(x', y')$ and thus we can conclude that both $[D]\neg\psi$ and $\langle D\rangle\psi$ belong to $\mathcal{L}(x', y')$ (contradiction).

$\mathcal{O}bs_D(\mathcal{L}(x', y')) \subseteq \mathcal{R}eq_D(\mathcal{L}(x, y))$ can analogously be proved by contradiction. □

Fulfilling compass structures are defined as follows.

Definition 7. *A compass φ-structure $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$ is said to be* fulfilling *if, for every point $(x, y) \in \mathbb{P}_\mathbb{S}$ and each formula $\psi \in \mathcal{R}eq_D(\mathcal{L}(x, y))$, there exists a point $(x', y') \sqsubset (x, y)$ in $\mathbb{P}_\mathbb{S}$ such that $\psi \in \mathcal{L}(x', y')$.*

Note that if $\mathcal{G}$ is fulfilling, then $\mathcal{R}eq_D(\mathcal{L}(x, x)) = \emptyset$ for all points "on the diagonal" $(x, x) \in \mathbb{P}_\mathbb{S}$.

We say that a compass φ-structure $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$ *features* a formula ψ if there exists a point $(x, y) \in \mathbb{P}_\mathbb{S}$ such that $\psi \in \mathcal{L}(x, y)$. The following result holds.

Proposition 8. *A* D*-formula φ is satisfiable iff there is a fulfilling compass φ-structure that features it.*

In a fulfilling compass φ-structure $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$, where $S = \{0, \ldots, t\}$, w.l.o.g., we will sometimes assume φ to be satisfied by the maximal interval $[0, t]$, that is, $\varphi \in \mathcal{L}(0, t)$.

The notion of homogeneous models directly transfers to compass structures.

Definition 9. *A compass φ-structure $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$ is* homogeneous *if, for every point $(x, y) \in \mathbb{P}_\mathbb{S}$ and each $p \in \mathcal{AP}$, we have that $p \in \mathcal{L}(x, y)$ iff $p \in \mathcal{L}(x', x')$ for all $x \leq x' \leq y$.*

Proposition 8 can be tailored to homogeneous compass structures as follows.

Proposition 10. *A* $\mathrm{D}|_{\mathcal{H}om}$*-formula φ is satisfiable iff there is a fulfilling homogeneous compass φ-structure that features it.*

3 Satisfiability of $\mathrm{D}|_{\mathcal{H}om}$ over finite linear orders

In this section, we devise a satisfiability checking procedure for $\mathrm{D}|_{\mathcal{H}om}$-formulas over finite linear orders, which will also allow us to easily derive a model checking algorithm for $\mathrm{D}|_{\mathcal{H}om}$ over finite Kripke structures. To start with, we show that there is a ternary relation between φ-atoms, that we denote by $=^{D_\varphi}\!\!\rightarrow$, such that if it holds among all atoms in consecutive positions of a compass φ-structure, then the structure is fulfilling. Hence, we may say that $=^{D_\varphi}\!\!\rightarrow$ is the rule for labeling fulfilling compasses. Next, we introduce an equivalence relation $\sim$ between *rows* of a compass φ-structure. Since it has finite index—exponentially bounded by $|\varphi|$—and it preserves fulfillment of compasses, it is intuitively possible to "contract" the structures when we can find two related rows. Moreover, any contraction done according to $\sim$ keeps the same atoms (only the number of their occurrences may vary), and thus if a compass features φ before the contraction, then φ is still featured after it. This fact is exploited to build a satisfiability algorithm for $\mathrm{D}|_{\mathcal{H}om}$-formulas which makes use of *polynomial working space* only, because (*i*) it only needs to keep track of two rows of a compass at a time, (*ii*) all rows satisfy some nice properties that make it possible to succinctly encode them, and (*iii*) compass contractions are implicitly performed by means of a reachability check in a suitable graph, whose nodes are the equivalence classes of $\sim$.

Let us now introduce the aforementioned ternary relation $=^{D_\varphi}\!\!\rightarrow$ among atoms.

Definition 11. *Given three φ-atoms A_1, A_2 and A_3, we say that A_3 is D_φ-generated by A_1, A_2 (written $A_1A_2 =^{D_\varphi}\!\!\rightarrow A_3$) if:* (*i*) $A_3 \cap \mathcal{AP} = A_1 \cap A_2 \cap \mathcal{AP}$ *and* (*ii*) $\mathcal{R}eq_D(A_3) = \mathcal{R}eq_D(A_1) \cup \mathcal{R}eq_D(A_2) \cup \mathcal{O}bs_D(A_1) \cup \mathcal{O}bs_D(A_2)$.

It is immediate to show that $A_1A_2 =^{D_\varphi}\!\!\rightarrow A_3$ iff $A_2A_1 =^{D_\varphi}\!\!\rightarrow A_3$ (i.e., the order of the first two components in the ternary relation is irrelevant). The next result, following from Proposition 4, proves that $=^{D_\varphi}\!\!\rightarrow$ expresses a *functional dependency* on φ-atoms.

Lemma 12. *Given two φ-atoms $A_1, A_2 \in \mathcal{A}_\varphi$, there exists* exactly one *φ-atom $A_3 \in \mathcal{A}_\varphi$ such that $A_1A_2 =^{D_\varphi}\!\!\rightarrow A_3$.*

Proof. Let us suppose by contradiction that there exist A_3 and A'_3 in $\mathcal{A}_\varphi$ such that $A_3 \neq A'_3$, $A_1A_2 =^{D_\varphi}\!\!\rightarrow A_3$ and $A_1A_2 =^{D_\varphi}\!\!\rightarrow A'_3$. By Definition 2 we can assume w.l.o.g. that there exists $\psi \in \mathrm{CL}(\varphi)$ such that $\psi \in A_3$ and $\neg\psi \in A'_3$. Moreover we choose ψ as a minimal formula that satisfies $\psi \in A_3$ and $\neg\psi \in A'_3$, i.e., each proper sub-formula ψ' of ψ either belongs to both A_3 and A'_3 or does not belong to either A_3 or A'_3.

Let us now prove that we get a contradiction. If $\psi = p$, with $p \in \mathcal{AP}$, by Definition 11 $A_3 \cap \mathcal{AP} = A_1 \cap A_2 \cap \mathcal{AP}$ and thus $p \in A_1 \cap A_2 \cap \mathcal{AP}$; since $A'_3 \cap \mathcal{AP} = A_1 \cap A_2 \cap \mathcal{AP}$, we have $p \in A'_3$. Hence, both p and $\neg p$ belong to A'_3 which contradicts Definition 2.

If $\psi = \neg\psi_1$, by the minimality of ψ, either $\psi_1 \in A_3 \cap A'_3$ or $\psi_1 \notin A_3 \cup A'_3$. In the former case we have $\neg\psi_1, \psi_1 \in A_3$ (contradiction). As for the latter, since we are assuming $\neg\psi \in A'_3$, we have $\neg\neg\psi_1 \in A'_3$, i.e., $\psi_1 \in A'_3$ (contradiction).

If $\psi = \psi_1 \vee \psi_2$, let us consider w.l.o.g. the case in which $\psi_1 \in A_3$. Since $\neg(\psi_1 \vee \psi_2) \in A'_3$ we have $\neg\psi_1 \in A'_3$ and thus $\psi_1 \notin A'_3$. However, by the minimality of ψ and since $\psi_1 \in A_3$, we have that $\psi_1 \in A'_3$ (contradiction).

Finally, if $\psi = \langle D\rangle\psi_1$ then $\neg\langle D\rangle\psi_1 \in A'_3$, hence $\psi_1 \notin \mathcal{R}eq_D(A'_3) = \mathcal{R}eq_D(A_1) \cup \mathcal{R}eq_D(A_2) \cup \mathcal{O}bs_D(A_1) \cup \mathcal{O}bs_D(A_2)$. Since $\psi \in A_3$ we have $\psi_1 \in \mathcal{R}eq_D(A_3) = \mathcal{R}eq_D(A_1) \cup \mathcal{R}eq_D(A_2) \cup \mathcal{O}bs_D(A_1) \cup \mathcal{O}bs_D(A_2)$ (contradiction). □

Definition 11 and Lemma 12 can be exploited to label a homogeneous compass φ-structure $\mathcal{G}$, namely, to determine the φ-atoms labeling all the points (x, y) of $\mathcal{G}$, starting from the ones on the diagonal. The idea is the following: if two φ-atoms A_1 and A_2 label respectively the greatest

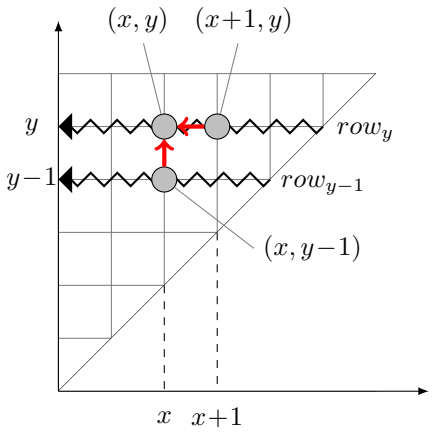

Figure 2: Rule for labeling homogeneous fulfilling compass φ-structures

proper prefix $[x, y-1]$, that is, the point $(x, y-1)$, and the greatest proper suffix $[x+1, y]$, that is, $(x+1, y)$, of the same interval $[x, y]$, then the atom A_3 labeling $[x, y]$ is unique, and it is precisely the one satisfying $A_1 A_2 {=}^{D_\varphi}\!\!\rightarrow A_3$ (see Figure 2). The next lemma proves that this is the general rule for labeling fulfilling homogeneous compasses.

Lemma 13. *Let $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$. $\mathcal{G}$ is a fulfilling homogeneous compass φ-structure iff, for every pair $x, y \in S$, we have: (i) $\mathcal{L}(x, y-1)\mathcal{L}(x+1, y) {=}^{D_\varphi}\!\!\rightarrow \mathcal{L}(x, y)$ if $x < y$, and (ii) $\mathcal{R}eq_D(\mathcal{L}(x, y)) = \emptyset$ if $x = y$.*

Proof. ($\Rightarrow$) Let us consider $x, y \in S$. First we note that, since $\mathcal{G}$ is fulfilling, it must be $\mathcal{R}eq_D(\mathcal{L}(x, y)) = \emptyset$ whenever $x = y$. Otherwise, if $x < y$, we consider the labellings $\mathcal{L}(x, y-1)$ and $\mathcal{L}(x{+}1, y)$. By the homogeneity property of Definition 9, $\mathcal{L}(x, y) \cap \mathcal{AP} = \mathcal{L}(x, y{-}1) \cap \mathcal{L}(x{+}1, y) \cap \mathcal{AP}$: condition (i) of Definition 11 holds. Moreover, since $\mathcal{G}$ is fulfilling, for every $\psi \in \mathcal{R}eq_D(\mathcal{L}(x, y))$ we have that either $\psi \in \mathcal{L}(x, y-1)$, or $\psi \in \mathcal{L}(x+1, y)$, or $\psi \in \mathcal{L}(x', y')$ for some $x < x' \leq y' < y$. In the first two cases $\psi \in \mathcal{O}bs_D(\mathcal{L}(x, y-1)) \cup \mathcal{O}bs_D(\mathcal{L}(x+1, y))$. As for the last case, by Lemma 6 $\mathcal{O}bs_D(\mathcal{L}(x', y')) \subseteq \mathcal{R}eq_D(\mathcal{L}(x, y-1))$ and $\mathcal{O}bs_D(\mathcal{L}(x', y')) \subseteq \mathcal{R}eq_D(\mathcal{L}(x+1, y))$, hence $\psi \in \mathcal{R}eq_D(\mathcal{L}(x, y-1))$ and $\psi \in \mathcal{R}eq_D(\mathcal{L}(x+1, y))$. We can conclude that $\mathcal{R}eq_D(\mathcal{L}(x, y)) \subseteq \mathcal{O}bs_D(\mathcal{L}(x, y-1)) \cup \mathcal{O}bs_D(\mathcal{L}(x+1, y)) \cup \mathcal{R}eq_D(\mathcal{L}(x, y-1)) \cup \mathcal{R}eq_D(\mathcal{L}(x+1, y))$. The converse inclusion ($\supseteq$) follows by Lemma 6, hence condition (ii) of Definition 11 holds. We conclude that $\mathcal{L}(x, y-1)\mathcal{L}(x+1, y) {=}^{D_\varphi}\!\!\rightarrow \mathcal{L}(x, y)$.

($\Leftarrow$) Let us consider $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$ such that, for every pair $x, y \in S$, $x \leq y$, we have $\mathcal{L}(x, y-1)\mathcal{L}(x+1, y) {=}^{D_\varphi}\!\!\rightarrow \mathcal{L}(x, y)$ if $x < y$, and $\mathcal{R}eq_D(\mathcal{L}(x, y)) = \emptyset$ if $x = y$. We have to prove that $\mathcal{G}$ is a homogeneous fulfilling compass φ-structure.

First, we prove consistency w.r.t. the relation D_φ. Let us show that, for all pairs of points (x, y) and (x', y') with $(x', y') \sqsubset (x, y)$, we have $\mathcal{L}(x, y)\ D_\varphi\ \mathcal{L}(x', y')$. The proof is by induction on $\Delta = (x' - x) + (y - y') \geq 1$. If $\Delta = 1$, either $(x', y') = (x+1, y)$ or $(x', y') = (x, y-1)$. Let us consider $(x', y') = (x{+}1, y)$ (the other case is symmetric). Since $\mathcal{L}(x, y{-}1)\mathcal{L}(x{+}1, y) {=}^{D_\varphi}\!\!\rightarrow \mathcal{L}(x, y)$, we easily get that $\mathcal{L}(x, y)\ D_\varphi\ \mathcal{L}(x{+}1, y)$. If $\Delta \geq 2$, since $(x', y') \sqsubset (x, y)$, then $(x', y'+1) \sqsubset (x, y)$ or $(x'-1, y') \sqsubset (x, y)$. We only consider $(x'-1, y') \sqsubset (x, y)$, being the other case symmetric. By the inductive hypothesis, $\mathcal{L}(x, y)\ D_\varphi\ \mathcal{L}(x'{-}1, y')$. Since $\mathcal{L}(x'{-}1, y'{-}1)\mathcal{L}(x', y') {=}^{D_\varphi}\!\!\rightarrow \mathcal{L}(x'{-}1, y')$, we have $\mathcal{L}(x'-1, y')\ D_\varphi\ \mathcal{L}(x', y')$. Let us observe that D_φ is a transitive relation, and thus $\mathcal{L}(x, y)\ D_\varphi\ \mathcal{L}(x', y')$.

Let us now show that $\mathcal{G}$ is fulfilling. We prove that for every point $(x, y) \in \mathbb{P}_{\mathbb{S}}$ and for every $\psi \in \mathcal{R}eq_D(\mathcal{L}(x, y))$, there exists $(x', y') \in \mathbb{P}_{\mathbb{S}}$, $(x', y') \sqsubset (x, y)$ such that $\psi \in \mathcal{L}(x', y')$. The proof is by induction on $y - x \geq 0$. If $x = y$, we have $\mathcal{R}eq_D(\mathcal{L}(x, y)) = \emptyset$, hence the thesis holds vacuously. If $y - x \geq 1$, since $\mathcal{L}(x, y-1)\mathcal{L}(x+1, y) \mathrel{=}D_\varphi\!\!\rightarrow \mathcal{L}(x, y)$, we have $\mathcal{R}eq_D(\mathcal{L}(x, y)) = \mathcal{R}eq_D(\mathcal{L}(x, y - 1)) \cup \mathcal{R}eq_D(\mathcal{L}(x + 1, y)) \cup \mathcal{O}bs_D(\mathcal{L}(x, y - 1)) \cup \mathcal{O}bs_D(\mathcal{L}(x + 1, y))$. If $\psi \in \mathcal{O}bs_D(\mathcal{L}(x, y - 1)) \cup \mathcal{O}bs_D(\mathcal{L}(x+1, y))$, the thesis is verified. If $\psi \in \mathcal{R}eq_D(\mathcal{L}(x+1, y))$ (the case $\psi \in \mathcal{R}eq_D(\mathcal{L}(x, y-1))$ is symmetric and thus omitted), by the inductive hypothesis, $\psi \in \mathcal{L}(x'', y'')$ for some $(x'', y'') \sqsubset (x + 1, y) \sqsubset (x, y)$.

It remains to prove that $\mathcal{G}$ is homogeneous. We have to show that, for every $(x, y) \in \mathbb{P}_{\mathbb{S}}$ and every $p \in \mathcal{AP}$, $p \in \mathcal{L}(x, y)$ iff for every point (x', x'), with $x \leq x' \leq y$, we have $p \in \mathcal{L}(x', x')$. The proof is by induction on the length of the interval (x, y). If $x = y$ the property trivially holds. Let us consider now $y - x > 0$ (inductive step). By the inductive hypothesis, since $(x + 1, y)$ and $(x, y - 1)$ are shorter than (x, y), we have $p \in \mathcal{L}(x + 1, y)$ (resp., $p \in \mathcal{L}(x, y - 1)$) iff, for every (x', x') with $x+1 \leq x' \leq y$, (resp., $x \leq x' \leq y-1$), $p \in \mathcal{L}(x', x')$. Thus $p \in \mathcal{L}(x+1, y) \cap \mathcal{L}(x, y-1)$ iff for every (x', x') with $x \leq x' \leq y$, $p \in \mathcal{L}(x', x')$. Since $\mathcal{L}(x + 1, y)\mathcal{L}(x, y - 1) \mathrel{=}D_\varphi\!\!\rightarrow \mathcal{L}(x, y)$, we have $\mathcal{L}(x, y) \cap \mathcal{AP} = \mathcal{L}(x + 1, y) \cap \mathcal{L}(x, y - 1) \cap \mathcal{AP}$. Therefore $p \in \mathcal{L}(x, y)$ iff for every (x', x'), with $x \leq x' \leq y$, we have $p \in \mathcal{L}(x', x')$. □

Now we introduce the concept of φ-row, which can be viewed as the ordered sequence of (the occurrences of) atoms labelling a row of a compass φ-structure. Given an atom $A \in \mathcal{A}_\varphi$, we call it *reflexive* if $A \; D_\varphi \; A$, *irreflexive* otherwise.

Definition 14. *A φ-row is a finite sequence of φ-atoms $row = A_0^{m_0} \cdots A_n^{m_n}$, where A^m stands for m repetitions of A, such that for each $0 \leq i \leq n$, we have that $m_i > 0$—if $m_i > 1$, then A_i is reflexive—and for each $0 \leq j < i$, it holds that $A_i \; D_\varphi \; A_j$, $A_i \neq A_j$, and $(A_j \cap \mathcal{AP}) \supseteq (A_i \cap \mathcal{AP})$. Moreover, $\mathcal{R}eq_D(A_0) = \emptyset$.*

The length of a φ-row $row = A_0^{m_0} \cdots A_n^{m_n}$ is defined as $|row| = \sum_{0 \leq i \leq n} m_i$, and for each $0 \leq j < |row|$, the j-th element, denoted by $row[j]$, is the j-th symbol in the word $A_0^{m_0} \cdots A_n^{m_n}$, e.g., $row[0] = A_0$, $row[m_0] = A_1$, ... We denote by $\mathcal{R}ows_\varphi$ the set of all possible φ-rows. This set may be infinite.

The number of distinct atoms in any φ-row is bounded. Since for each $0 \leq i \leq n$ and each $0 \leq j < i$, $A_i \; D_\varphi \; A_j$, it holds that $\mathcal{R}eq_D(A_j) \subseteq \mathcal{R}eq_D(A_i)$. Therefore, two monotonic sequences for every φ-row can be considered, one increasing, i.e., $\emptyset = \mathcal{R}eq_D(A_0) \subseteq \mathcal{R}eq_D(A_1) \subseteq \ldots \subseteq \mathcal{R}eq_D(A_n)$, and one decreasing, i.e., $(A_0 \cap \mathcal{AP}) \supseteq (A_1 \cap \mathcal{AP}) \supseteq \ldots \supseteq (A_n \cap \mathcal{AP})$. The number of distinct elements is bounded by $|\varphi|$ in the former sequence and by $|\varphi| + 1$ in the latter (as $|\,\mathrm{REQ}_\varphi\,| \leq |\varphi| - 1$ and $|\mathcal{AP}| \leq |\varphi|$–w.l.o.g., we can consider only the letters actually occurring in φ). Since, as already shown (Proposition 4), a set of requests and a set of proposition letters uniquely determine a φ-atom, any φ-row may feature at most $2|\varphi|$ distinct atoms, i.e., $n < 2|\varphi|$.

Given a homogeneous compass φ-structure $\mathcal{G} = (\mathbb{P}_{\mathbb{S}}, \mathcal{L})$, for every $y \in S$, we define row_y as the word of φ-atoms $row_y = \mathcal{L}(y, y) \cdots \mathcal{L}(0, y)$, i.e., the sequence of atoms labeling points of $\mathcal{G}$ with the same y-coordinate, starting from the one on the diagonal inwards (see Figure 2).

Lemma 15. *Let $\mathcal{G} = (\mathbb{P}_{\mathbb{S}}, \mathcal{L})$ be a fulfilling homogeneous compass φ-structure. For every $y \in S$, row_y is a φ-row.*

Proof. Let $row_y = \mathcal{L}(y, y)^{m_0}\mathcal{L}(y-m_0, y)^{m_1} \cdots \mathcal{L}(y-\sum_{0 \leq i < n} m_i, y)^{m_n}$ where, for every $0 \leq j \leq n$, $\mathcal{L}(y - \sum_{0 \leq i < j} m_j, y)^{m_j}$ is a maximal substring of identical atoms (note that any row_y can be represented w.l.o.g. in this way, for $m_i > 0$). Since $(y, y) \sqsubset \ldots \sqsubset (0, y)$, by Lemma 6, $\mathcal{R}eq_D(\mathcal{L}(y, y)) \subseteq \mathcal{R}eq_D(\mathcal{L}(y - m_0, y)) \subseteq \ldots \subseteq \mathcal{R}eq_D(\mathcal{L}(y - \sum_{0 \leq i < n} m_i, y))$. Moreover, by homogeneity, $(\mathcal{L}(y, y) \cap \mathcal{AP}) \supseteq (\mathcal{L}(y - m_0, y) \cap \mathcal{AP}) \supseteq \ldots \supseteq (\mathcal{L}(y - \sum_{0 \leq i < n} m_i, y) \cap \mathcal{AP})$. By

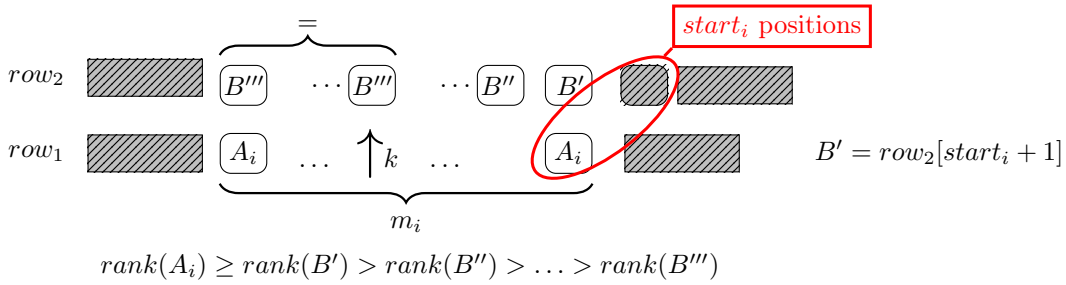

Figure 3: A graphical account of the proof of Lemma 18.

maximality, $\mathcal{L}(y - \sum_{0 \leq i < j} m_i, y) \neq \mathcal{L}(y - \sum_{0 \leq i < j-1} m_i, y)$ for every $0 < j \leq n$, and thus, since φ-atoms are uniquely determined by a pair $R \subseteq \mathrm{REQ}_\varphi$ and $P \subseteq \mathcal{AP}$ which are monotonically arranged, we can conclude that $\mathcal{L}(y - \sum_{0 \leq i < j} m_i, y) \neq \mathcal{L}(y - \sum_{0 \leq i < j'} m_i, y)$ for every $j' < j$. Now we prove that $m_j = 1$ if $\mathcal{L}(y - \sum_{0 \leq i < j} m_i, y)$ is irreflexive. By contradiction let us suppose that $m_j > 1$; then $\mathcal{L}(y - \sum_{0 \leq i < j} m_i, y) = \mathcal{L}(y - (\sum_{0 \leq i < j} m_i) - 1, y)$. Since $\mathcal{L}(y - (\sum_{0 \leq i < j} m_i) - 1, y)\ D_\varphi\ \mathcal{L}(y - \sum_{0 \leq i < j} m_i, y)$, then $\mathcal{L}(y - \sum_{0 \leq i < j} m_i, y)$ is reflexive (contradiction). Finally we have $\mathcal{R}eq_D(\mathcal{L}(y, y)) = \emptyset$, as $\mathcal{G}$ is fulfilling. □

We now define the *successor* relation between pairs of φ-rows, denoted as $=^{row_\varphi}\!\!\rightarrow$, which is basically a component-wise application of $=^{D_\varphi}\!\!\rightarrow$ over the elements of two φ-rows (remember that atoms on rows are collected from right to left).

Definition 16. *Given two φ-rows row and row', we say that row' is a* successor *of row, or $row =^{row_\varphi}\!\!\rightarrow row'$, if $|row'| = |row| + 1$, and for all $0 \leq i < |row|$, $row[i]row'[i] =^{D_\varphi}\!\!\rightarrow row'[i+1]$.*

The next lemma states that consecutive rows in homogeneous fulfilling compass φ-structures respect the successor relation.

Lemma 17. *Let $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$, with $\mathcal{R}eq_D(\mathcal{L}(x, x)) = \emptyset$ for all $(x, x) \in \mathbb{P}_\mathbb{S}$. $\mathcal{G}$ is a fulfilling homogeneous compass φ-structure iff, for each $0 \leq y < |S| - 1$, $row_y =^{row_\varphi}\!\!\rightarrow row_{y+1}$.*

Proof. ($\Rightarrow$) By Lemma 15, the rows $row_0, \ldots, row_{|S|-1}$ of $\mathcal{G}$ are φ-rows. By Lemma 13, for every $0 \leq x \leq y$, $\mathcal{L}(x, y)\mathcal{L}(x+1, y+1) =^{D_\varphi}\!\!\rightarrow \mathcal{L}(x, y+1)$. Since $\mathcal{L}(x, y) = row_y[y - x]$, $\mathcal{L}(x+1, y+1) = row_{y+1}[(y+1) - (x+1)]$, and $\mathcal{L}(x, y+1) = row_{y+1}[(y+1) - x]$ we can conclude that $row_y =^{row_\varphi}\!\!\rightarrow row_{y+1}$.

($\Leftarrow$) Since for each $0 \leq y < |S| - 1$, $row_y =^{row_\varphi}\!\!\rightarrow row_{y+1}$, we have that for all $0 \leq i \leq y$, $row_y[i]row_{y+1}[i] =^{D_\varphi}\!\!\rightarrow row_{y+1}[i+1]$, namely, $\mathcal{L}(y - i, y)\mathcal{L}(y + 1 - i, y + 1) =^{D_\varphi}\!\!\rightarrow \mathcal{L}(y - i, y + 1)$. Let $x = y - i$, for $0 \leq x \leq y$. We get $\mathcal{L}(x, y)\mathcal{L}(x+1, y+1) =^{D_\varphi}\!\!\rightarrow \mathcal{L}(x, y+1)$. By Lemma 13, $\mathcal{G}$ is a fulfilling homogeneous compass φ-structure. □

Given an atom $A \in \mathcal{A}_\varphi$, we define the *rank of A*, written $rank(A)$, as $|\,\mathrm{REQ}_\varphi\,| - |\mathcal{R}eq_D(A)|$. Clearly, $rank(A) < |\varphi|$. Whenever $A\ D_\varphi\ A'$, for some $A' \in \mathcal{A}_\varphi$, $\mathcal{R}eq_D(A') \subseteq \mathcal{R}eq_D(A)$, and hence $rank(A) \leq rank(A')$ and $|\mathcal{R}eq_D(A) \setminus \mathcal{R}eq_D(A')| \leq rank(A')$. We can see the *rank* of an atom as the "number of degrees of freedom" that it gives to the atoms that stay "above it". In particular, by definition, for every φ-row $row = A_0^{m_0} \cdots A_n^{m_n}$, we have $rank(A_0) \geq \ldots \geq rank(A_n)$. The next result uses the notion of rank to provide an insight on how consecutive φ-rows are connected (see Figure 3).

Lemma 18. *Let row_1, row_2 be two φ-rows, with $row_1 = A_0^{m_0} \cdots A_n^{m_n}$ and $row_1 \mathrel{=}^{row_\varphi}\!\!\rightarrow row_2$. For each $0 \leq i \leq n$, let $start_i = \sum_{0 \leq j < i} m_j$. If $m_i > rank(A_i)$, then there exists $start_i < k \leq start_i + m_i$ such that:*

(i) $row_2[k]$ is reflexive;

(ii) $rank(row_2[j]) > rank(row_2[j+1])$ for each $start_i < j < k$;

(iii) $row_2[j] = row_2[j+1]$ for each $k \leq j < start_i + m_i$;

(iv) if m' is the exponent of the atom $row_2[k]$, then $m' > rank(row_2[k])$.

Proof. If $m_i = 1$, by hypothesis we have $rank(A_i) = 0$. Hence, $rank(row_2[start_i + 1]) = 0$, because $row_1 \mathrel{=}^{row_\varphi}\!\!\rightarrow row_2$, and thus $row_2[start_i + 1]$ is (trivially) reflexive. All claims hold by choosing $k = start_i + 1$.

Let us then assume $m_i > 1$. First, we prove that for each $start_i < j \leq start_i + m_i$, if $row_2[j]$ is reflexive, then for each $j \leq j' \leq start_i + m_i$, $row_2[j'] = row_2[j]$. If $j = start_i + m_i$ there is nothing to prove. Thus, let us consider $j < start_i + m_i$. Since we are assuming that $row_2[j]$ is reflexive, then $\mathcal{O}bs_D(row_2[j]) \subseteq \mathcal{R}eq_D(row_2[j])$. Since $row_1 \mathrel{=}^{row_\varphi}\!\!\rightarrow row_2$, we have that $\mathcal{R}eq_D(A_i), \mathcal{O}bs_D(A_i) \subseteq \mathcal{R}eq_D(row_2[j])$, and $\mathcal{R}eq_D(row_2[j+1]) = \mathcal{R}eq_D(row_2[j]) \cup \mathcal{O}bs_D(row_2[j]) \cup \mathcal{R}eq_D(A_i) \cup \mathcal{O}bs_D(A_i) = \mathcal{R}eq_D(row_2[j])$. Moreover, again from $row_1 \mathrel{=}^{row_\varphi}\!\!\rightarrow row_2$, we have that $row_2[j] \cap \mathcal{AP} = row_2[j-1] \cap A_i \cap \mathcal{AP}$ and $row_2[j+1] \cap \mathcal{AP} = row_2[j] \cap A_i \cap \mathcal{AP} = row_2[j-1] \cap A_i \cap \mathcal{AP}$. Thus, $row_2[j+1] = row_2[j]$, because the two atoms feature exactly the same requests and proposition letters (Proposition 4). Then, since $A_i\ row_2[j] \mathrel{=}^{D_\varphi}\!\!\rightarrow row_2[j+1]$, by iterating the reasoning and exploiting Lemma 12 we can conclude that $row_2[j] = row_2[j']$ for each $j \leq j' \leq start_i + m_i$.

Now, it can be easily shown that if we have two atoms A and A' such that $A\ D_\varphi\ A'$ and A' is irreflexive, then $rank(A) < rank(A')$, and we have just proved that we cannot interleave reflexive atoms with irreflexive ones "above" the A_i's (all irreflexive atoms must "come before" reflexive ones in the part of row_2 "above" the A_i's). Thus, in the worst possible case, the atoms $row_2[start_i+1], \ldots, row_2[start_i+rank(A_i)]$ may be irreflexive (as $rank(row_2[start_i+1]) > \ldots > rank(row_2[start_i+rank(A_i)])$ and $rank(A_i) \geq rank(row_2[start_i+1])$). Note that these irreflexive atoms may be the "first" $rank(A_i)$ atoms above the A_i's only, and not the "first" $rank(A_i)+1$, since any atom with rank equal to 0 is reflexive. We conclude that $row_2[start_i + rank(A_i) + 1]$ must be reflexive. Thus, we can choose $k = start_i + rank(A_i) + 1$. Since by hypothesis $m_i \geq rank(A_i) + 1$, we get that $start_i < k \leq start_i + m_i$.

As for the last claim, we have that $rank(row_2[k]) \leq rank(row_2[start_i+1]) - (k - start_i - 1) \leq rank(A_i) - (k - start_i - 1)$. Then, the exponent m' of $row_2[k]$ is such that $m' \geq m_i - (rank(A_i) - rank(row_2[k]))$, that is, at least $m_i - (rank(A_i) - rank(row_2[k]))$ atoms labelled by $row_2[k]$ occur in the block $start_i+1, \ldots, start_i+m_i$ of row_2 (see Figure 3). Since by hypothesis $m_i > rank(A_i)$, then $m_i - rank(A_i) > 0$ and $rank(row_2[k]) < m'$. □

Now we introduce an equivalence relation $\sim$ over $\mathcal{R}ows_\varphi$ which is the key ingredient of the proofs showing that both satisfiability and MC for $\mathrm{D}|_{\mathcal{H}om}$-formulas are decidable.

Definition 19. *Given two φ-rows $row_1 = A_0^{m_0} \cdots A_n^{m_n}$ and $row_2 = \hat{A}_0^{\hat{m}_0} \cdots \hat{A}_{\hat{n}}^{\hat{m}_{\hat{n}}}$, we say that they are* equivalent, *written $row_1 \sim row_2$, if (i) $n = \hat{n}$, and (ii) for each $0 \leq i \leq n$, $A_i = \hat{A}_i$, and $m_i = \hat{m}_i$ or both m_i and $\hat{m}_i$ are (strictly) greater than $rank(A_i)$.*

Note that if two rows feature the same set of atoms, the lower the rank of an atom A_i, the lower the number of occurrences of A_i both the rows have to feature in order to belong to the same equivalence class. As an example, let row_1 and row_2 be two rows with $row_1 = A_0^{m_0} A_1^{m_1}$,

$row_2 = A_0^{\overline{m}_0} A_1^{\overline{m}_1}$, $rank(A_0) = 4$, and $rank(A_1) = 3$. If $m_1 = 4$ and $\overline{m}_1 = 5$ they are both greater than $rank(A_1)$, and hence they do not violate the condition for $row_1 \sim row_2$. On the other hand, if $m_0 = 4$ and $\overline{m}_0 = 5$, we have that m_0 is less than or equal to $rank(A_0)$. Thus, in this case, $row_1 \not\sim row_2$ due to the indexes of A_0. This happens because $rank(A_0)$ is greater than $rank(A_1)$. Two cases in which $row_1 \sim row_2$ are $m_0 = \overline{m}_0$ and $m_0, \overline{m}_0 \geq 5$.

The relation $\sim$ has finite index, which is roughly bounded by the number of all the possible φ-rows $row = A_0^{m_0} \cdots A_n^{m_n}$, with exponents m_i ranging from 1 to $|\varphi|$. Since (i) the number of possible atoms is $2^{|\varphi|}$, (ii) the number of *distinct* atoms in any φ-row is at most $2|\varphi|$, and (iii) the number of possible functions $f : \{1, \ldots, \ell\} \to \{1, \ldots, |\varphi|\}$ is $|\varphi|^\ell$, we have that the number of distinct equivalence classes of $\sim$ is bounded by

$$\sum_{j=1}^{2|\varphi|} (2^{|\varphi|})^j \cdot |\varphi|^j \leq 2^{3|\varphi|^2},$$

which is exponential in the length of the input formula φ. We denote the set of the equivalence classes of $\sim$ over all the possible φ-rows by $\mathcal{R}ows_\varphi^\sim$.

Now we extend the relation ${}^{=row_\varphi}\!\!\rightarrow$ to equivalence classes of $\sim$ in the following way.

Definition 20. *Given two φ-row classes $[row_1]_\sim$ and $[row_2]_\sim$, we say that $[row_2]_\sim$ is a successor of $[row_1]_\sim$, written $[row_1]_\sim {}^{=row_\varphi}\!\!\rightarrow [row_2]_\sim$, if there exist $row_1' \in [row_1]_\sim$ and $row_2' \in [row_2]_\sim$ such that $row_1' {}^{=row_\varphi}\!\!\rightarrow row_2'$.*

The following result proves that if some $row_1' \in [row_1]_\sim$ has a successor in $[row_2]_\sim$, then *every* φ*-row* of $[row_1]_\sim$ has a successor in $[row_2]_\sim$.

Lemma 21. *Given two φ-row classes $[row_1]_\sim$ and $[row_2]_\sim$ such that $[row_1]_\sim {}^{=row_\varphi}\!\!\rightarrow [row_2]_\sim$, for every $row \in [row_1]_\sim$ there exists $row' \in [row_2]_\sim$ such that $row {}^{=row_\varphi}\!\!\rightarrow row'$.*

The proof, omitted for space reasons (it can be found in Appendix A.1), begins by considering two φ-rows, row and $\overline{row}$, such that $row \in [row_1]_\sim$, $\overline{row} \in [row_2]_\sim$, and $row {}^{=row_\varphi}\!\!\rightarrow \overline{row}$ (such a pair always exists by Definition 20). Then, we consider another φ-row, $row' \neq row$ in $[row_1]_\sim$, and we show (constructively) how to build $\overline{row}' \in [row_2]_\sim$ such that $row' {}^{=row_\varphi}\!\!\rightarrow \overline{row}'$. This is sufficient to prove the claim: $\overline{row}'$ is built by making use of the facts that $row' \sim row$ and $row {}^{=row_\varphi}\!\!\rightarrow \overline{row}$, and of the properties stated by Lemma 18.

The following result arranges the equivalence classes $\mathcal{R}ows_\varphi^\sim$ in a graph $G_{\varphi\sim}$.

Definition 22. *Let φ be a $\mathrm{D}|_{\mathcal{H}om}$-formula. The φ $\sim$*graph *of φ is $G_{\varphi\sim} = (\mathcal{R}ows_\varphi^\sim, {}^{=row_\varphi}\!\!\rightarrow)$.*

The next theorem reduces the problem of satisfiability checking for a $\mathrm{D}|_{\mathcal{H}om}$-formula φ over finite linear orders (equivalent, by Proposition 10, to deciding if there is a homogeneous fulfilling compass φ-structure that features φ) to a reachability problem in the φ $\sim$graph, allowing us to determine the computational complexity of the former problem.

Theorem 23. *Given a $\mathrm{D}|_{\mathcal{H}om}$-formula φ, there exists a homogeneous fulfilling compass φ-structure $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$ that features φ iff there exists a path in $G_{\varphi\sim} = (\mathcal{R}ows_\varphi^\sim, {}^{=row_\varphi}\!\!\rightarrow)$ from some class $[row]_\sim \in \mathcal{R}ows_\varphi^\sim$ to some class $[row']_\sim \in \mathcal{R}ows_\varphi^\sim$ such that (1) there exists $row_1 \in [row]_\sim$ with $|row_1| = 1$, and (2) there exist $row_2 \in [row']_\sim$ and $0 \leq i < |row_2|$ such that $\varphi \in row_2[i]$.*

Proof. Preliminarily we observe that, in (1), if $|row_1| = 1$, then $\{row_1\} = [row]_\sim$; moreover, in (2), if for $row_2 \in [row']_\sim$ and $0 \leq i < |row_2|$ we have that $\varphi \in row_2[i]$, then for any $row_2' \in [row']_\sim$, there is $0 \leq i' < |row_2'|$ such that $\varphi \in row_2'[i']$.

($\Rightarrow$) Let us consider a homogeneous fulfilling compass φ-structure $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$ that features φ. By Lemmata 15 and 17, $\mathcal{L}(0,0) =^{row_\varphi}\!\!\rightarrow row_1 =^{row_\varphi}\!\!\rightarrow \cdots =^{row_\varphi}\!\!\rightarrow row_{\max(S)}$. Thus there exist two indexes $0 \leq j \leq \max(S)$ and $0 \leq i < |row_j|$ for which $\varphi \in row_j[i]$. By Definition 20, we get that $[\mathcal{L}(0,0)]_\sim =^{row_\varphi}\!\!\rightarrow [row_1]_\sim =^{row_\varphi}\!\!\rightarrow \cdots =^{row_\varphi}\!\!\rightarrow [row_j]_\sim$ is a path in $G_{\varphi\sim}$; it is immediate to check that it fulfils requirements (1) and (2).
($\Leftarrow$) Let us assume there is a path $[row_0]_\sim =^{row_\varphi}\!\!\rightarrow \cdots =^{row_\varphi}\!\!\rightarrow [row_m]_\sim$ in $G_{\varphi\sim} = (\mathcal{R}ows^\sim_\varphi, =^{row_\varphi}\!\!\rightarrow)$ for which $|row_0| = 1$ and there exists i such that $\varphi \in row_m[i]$. By applying repeatedly Lemma 21 we get that there exists a sequence $row'_0 =^{row_\varphi}\!\!\rightarrow \cdots =^{row_\varphi}\!\!\rightarrow row'_m$ of φ-rows where $row'_0 = row_0$, for every $0 \leq j \leq m$, $row'_j \in [row_j]_\sim$, and there exists i' such that $\varphi \in row'_m[i']$. We observe that, by Definition 16, $|row'_j| = |row'_{j-1}| + 1$ for $1 \leq j \leq m$ and, since $|row'_0| = 1$, we have $|row'_j| = j + 1$. Let us now define $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$ where $S = \{0, \ldots, m\}$ and $\mathcal{L}(x, y) = row'_y[y - x]$ for every $0 \leq x \leq y \leq m$. By Lemma 17, $\mathcal{G}$ is a fulfilling homogeneous compass φ-structure. Finally, since $\varphi \in row'_m[i']$, $\mathcal{G}$ features φ. □

The size of $G_{\varphi\sim} = (\mathcal{R}ows^\sim_\varphi, =^{row_\varphi}\!\!\rightarrow)$ is bounded by $|\mathcal{R}ows^\sim_\varphi|^2$, which is exponential in $|\varphi|$. However, it is possible to (non-deterministically) perform a reachability in $G_{\varphi\sim}$ by using space *logarithmic* in $|\mathcal{R}ows^\sim_\varphi|^2$. The *non-deterministic* procedure of Figure 4 exploits this fact in order to decide the satisfiability of a D$|_{\mathcal{H}om}$-formula φ, by using only a working space *polynomial* in $|\varphi|$: it searches for a suitable path in $G_{\varphi\sim}$, $[row_0]_\sim =^{row_\varphi}\!\!\rightarrow \cdots =^{row_\varphi}\!\!\rightarrow [row_m]_\sim$, where $row_0 = A$ for $A \in \mathcal{A}_\varphi$ with $\mathcal{R}eq_D(A) = \emptyset$, $m < M$, and $\varphi \in row_m[i]$ for $0 \leq i < |row_m|$. At the j-th iteration of line 4., row_j is non-deterministically generated, and it is checked whether $row_{j-1} =^{row_\varphi}\!\!\rightarrow row_j$. The procedure terminates after at most M iterations, where M is the maximum possible length of a simple path in $G_{\varphi\sim}$.

The working space used by the procedure is polynomial: M and *step* (which ranges in $[0, M-1]$) can be encoded in binary with $\lceil \log_2 M \rceil + 1 = O(|\varphi|^2)$ bits. At each step, we need to keep track of two φ-rows at a time, the current one, *row*, and its successor, *row*′: each φ-row can be represented as a sequence of at most $2|\varphi|$ (distinct) atoms, each one with an exponent that, by construction, cannot exceed M. Moreover, each φ-atom A can be represented using exactly $|\varphi|$ bits (for each $\psi \in \mathrm{CL}(\varphi)$, we set a bit to 1 if $\psi \in A$, and to 0 if $\neg\psi \in A$). Hence a φ-row can be encoded using $2|\varphi| \cdot (|\varphi| + \lceil \log_2 M \rceil + 1) = O(|\varphi|^3)$ bits. Finally, the condition $row =^{row_\varphi}\!\!\rightarrow row'$ can be checked by $O(|\varphi|^2)$ bits of space once we have guessed *row*′. This analysis entails the following result (we recall that **NPSPACE** = **PSPACE**).

Theorem 24. *The satisfiability problem for* D$|_{\mathcal{H}om}$*-formulas over finite linear orders is in* ***PSPACE****.*

We now outline which are the modifications to the previous concepts needed for proving the

Input: a D$|_{\mathcal{H}om}$-formula φ

1. Put $M \leftarrow 2^{3|\varphi|^2}$, $step \leftarrow 0$ and $row \leftarrow A$ for some atom $A \in \mathcal{A}_\varphi$ with $\mathcal{R}eq_D(A) = \emptyset$.
2. If there exists $0 \leq i < |row|$ such that $\varphi \in row[i]$, return **satisfiable**.
3. If $step = M - 1$, return **unsatisfiable**.
4. Non-deterministically generate a φ-row row' and check that $row =^{row_\varphi}\!\!\rightarrow row'$.
5. Put $step \leftarrow step + 1$ and $row \leftarrow row'$.
6. Go back to 2.

Figure 4: Non-deterministic procedure deciding the satisfiability of a D$|_{\mathcal{H}om}$-formula φ

decidability of satisfiability for $\mathrm{D}|_{\mathcal{H}om}$ with the strict relation $\sqsubset$, in place of $\sqsubseteq$. It is sufficient to replace the definitions of $=^{D_\varphi}\!\!\rightarrow$, φ-*row* and $=^{row_\varphi}\!\!\rightarrow$ with the following ones. For the sake of simplicity, we introduce a dummy atom $\boxdot$, for which we assume $\mathcal{R}eq_D(\boxdot) = \mathcal{O}bs_D(\boxdot) = \emptyset$.

Definition 25. *Given $A_1, A_3, A_4 \in \mathcal{A}_\varphi$ and $A_2 \in \mathcal{A}_\varphi \cup \{\boxdot\}$, we say that A_4 is D_φ $\sqsubset$-generated by A_1, A_2, A_3, written $A_1, A_2, A_3 =^{D_\varphi \sqsubset}\!\!\Rightarrow A_4$ iff (i) $A_4 \cap \mathcal{AP} = A_1 \cap A_3 \cap \mathcal{AP}$ and (ii) $\mathcal{R}eq_D(A_4) = \mathcal{R}eq_D(A_1) \cup \mathcal{R}eq_D(A_3) \cup \mathcal{O}bs_D(A_2)$.*

The idea of this definition is that, if an interval $[x, y]$, with $x < y$, is labeled by A_4, and the three subintervals $[x, y-1]$, $[x+1, y-1]$, and $[x+1, y]$ by A_1, A_2, A_3, resp., we want $A_1, A_2, A_3 =^{D_\varphi \sqsubset}\!\!\Rightarrow A_4$. In particular, if $x = y - 1$, then $A_2 = \boxdot$ (because $[x+1, y-1]$ is not a valid interval). Note that only $[x+1, y-1] \sqsubset [x, y]$, hence we want $\mathcal{O}bs_D(A_2) \subseteq \mathcal{R}eq_D(A_4)$; moreover, since the requests of A_1 and A_3 are fulfilled by a strict subinterval of $[x, y]$, it must be $\mathcal{R}eq_D(A_1) \subseteq \mathcal{R}eq_D(A_4)$ and $\mathcal{R}eq_D(A_3) \subseteq \mathcal{R}eq_D(A_4)$.

Definition 26. *A φ-$\sqsubset$-row is a finite sequence of φ-atoms $row = A_0^{m_0} \cdots A_n^{m_n}$ such that for every $0 \leq i \leq n$ we have $m_i > 0$, and for every $0 \leq j < i$, $\mathcal{R}eq_D(A_j) \subseteq \mathcal{R}eq_D(A_i)$, $A_i \neq A_j$, and $(A_j \cap \mathcal{AP}) \supseteq (A_i \cap \mathcal{AP})$. Moreover $\mathcal{R}eq_D(A_0) = \emptyset$.*

Definition 27. *Given two φ-rows row and row', we say that row' is a successor of row, denoted as $row =^{row_\varphi \sqsubset}\!\!\Rightarrow row'$, if $|row'| = |row| + 1$, and for every $0 \leq i < |row|$, $row[i]row[i-1]row'[i] =^{D_\varphi \sqsubset}\!\!\Rightarrow row'[i+1]$, where we assume $row[i-1] = \boxdot$ if $i = 0$.*

We conclude the section by stating the **PSPACE**-completeness of satisfiability for $\mathrm{D}|_{\mathcal{H}om}$ over finite linear orders (under both the *strict* and the *proper* semantic variants). The hardness proof can be found in Appendix A.3.

Theorem 28. *The satisfiability problem for $\mathrm{D}|_{\mathcal{H}om}$-formulas over finite linear orders is **PSPACE**-complete.*

4 Model checking for $\mathrm{D}|_{\mathcal{H}om}$ over Kripke structures

In this section we focus our attention on the *model checking (MC)* problem for $\mathrm{D}|_{\mathcal{H}om}$, namely, the problem of checking whether some behavioural properties, expressed as $\mathrm{D}|_{\mathcal{H}om}$-formulas, are satisfied by a model of a given system. The typical models are *Kripke structures*, which will now be introduced along with the semantic definition of $\mathrm{D}|_{\mathcal{H}om}$ over them.

Definition 29. *A* finite Kripke structure *is a tuple $\mathcal{K} = (\mathcal{AP}, W, E, \mu, s_0)$, where $\mathcal{AP}$ is a finite set of proposition letters, W is a finite set of states, $E \subseteq W \times W$ is a left-total relation between states, $\mu : W \to 2^{\mathcal{AP}}$ is a total labelling function, and $s_0 \in W$ is the initial state.*

For all $s \in W$, $\mu(s)$ is the set of proposition letters that hold on s, while E is the transition relation that describes the evolution of the system over time.

Figure 5 depicts the finite Kripke structure $\mathcal{K}_2 = (\{p, q\}, \{s_0, s_1\}, E, \mu, s_0)$, with $E = \{(s_0, s_0), (s_0, s_1), (s_1, s_0), (s_1, s_1)\}$, $\mu(s_0) = \{p\}$, and $\mu(s_1) = \{q\}$. The initial state s_0 is identified by a double circle.

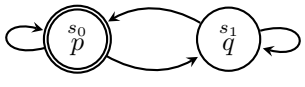

Figure 5: Kripke structure $\mathcal{K}_2$.

Definition 30. *A* trace ρ *of a finite Kripke structure* $\mathcal{K} = (\mathcal{AP}, W, E, \mu, s_0)$ *is a finite sequence of states* $s_1 \cdots s_n$*, with* $n \geq 1$*, such that* $(s_i, s_{i+1}) \in E$ *for* $i = 1, \ldots, n-1$.

For any trace $\rho = s_1 \cdots s_n$, we define: (i) $|\rho| = n$, and for $0 \leq i \leq |\rho| - 1$, $\rho(i) = s_{i+1}$; (ii) $\rho(i,j) = s_{i+1} \cdots s_{j+1}$, for $0 \leq i \leq j \leq |\rho| - 1$, is the subtrace of ρ bounded by i and j. Finally, if the first state of ρ is s_0 (the initial state of $\mathcal{K}$), ρ is called an *initial trace*.

Definition 31. *The interval model* $\mathbf{M}_\rho = \langle \mathbb{I}(\mathbb{S}), \circ, \mathcal{V} \rangle$ induced by a trace ρ *of a finite Kripke structure* $\mathcal{K} = (\mathcal{AP}, W, E, \mu, s_0)$ *is the homogeneous interval model such that:*
(i) $S = \{0, \ldots, |\rho| - 1\}$*, and* (ii) *for all* $x \in S$ *and* $p \in \mathcal{AP}$*:* $[x, x] \in \mathcal{V}(p)$ *iff* $p \in \mu(\rho(x))$.

Definition 32. *Let* $\mathcal{K}$ *be a finite Kripke structure and* ψ *be a* $\mathrm{D}|_{\mathcal{H}om}$*-formula. We say that a trace* $\rho(i,j)$ *of* $\mathcal{K}$ *satisfies* ψ*, denoted as* $\mathcal{K}, \rho(i,j) \models \psi$*, iff* $\mathbf{M}_\rho, [i,j] \models \psi$*. Moreover, we say that* $\mathcal{K}$ *models* ψ*, written* $\mathcal{K} \models \psi$*, iff for all* initial *traces* ρ' *of* $\mathcal{K}$*, it holds that* $\mathcal{K}, \rho' \models \psi$*. The* MC problem *for* $\mathrm{D}|_{\mathcal{H}om}$ *over finite Kripke structures is the problem of deciding if* $\mathcal{K} \models \psi$.

Note that $p \in \mathcal{AP}$ holds over $\rho = s_1 \cdots s_n$ iff it holds over all the states $s_1, \ldots, s_n$ of ρ (*homogeneity assumption*). Since the number of initial traces of $\mathcal{K}$ is infinite, MC for $\mathrm{D}|_{\mathcal{H}om}$ over Kripke structures is not trivially decidable.

We now describe how, with a slight modification of the previous satisfiability procedure, it is possible to derive a MC algorithm for $\mathrm{D}|_{\mathcal{H}om}$-formulas φ over finite Kripke structures $\mathcal{K}$. The idea is to consider some finite linear orders—not all the possible ones, unlike the case of satisfiability—precisely those corresponding to (some) initial traces of $\mathcal{K}$, checking whether $\neg\varphi$ holds over them: in such a case we have found a counterexample, and we can conclude that $\mathcal{K} \not\models \varphi$. To ensure this kind of "satisfiability driven by the traces of $\mathcal{K}$", we make a product between $\mathcal{K}$ and the previous graph $G_{\varphi\sim}$, getting what we call a "$(\varphi \sim \mathcal{K})$*-graph*". In the following, we will also exploit the notion of "compass structure *induced by a trace* ρ of $\mathcal{K}$", which is a fulfilling homogeneous compass φ-structure built from ρ and completely determined by it.

Given a finite Kripke structure $\mathcal{K} = (\mathcal{AP}, W, E, \mu, s_0)$ and a $\mathrm{D}|_{\mathcal{H}om}$-formula φ, we consider the $(\varphi \sim \mathcal{K})$-graph $G_{\varphi\sim\mathcal{K}}$, which is basically the product of $\mathcal{K}$ and $G_{\varphi\sim} = (\mathcal{R}ows^{\sim}_{\varphi}, {}^{=row_\varphi}\!\!\Rightarrow)$, formally defined as: $G_{\varphi\sim\mathcal{K}} = (\Gamma, \Xi)$, where:

- Γ is the maximal subset of $W \times \mathcal{R}ows^{\sim}_{\varphi}$ s.t.: if $(s, [row]_\sim) \in \Gamma$ then $\mu(s) = row[0] \cap \mathcal{AP}$;
- $\big((s_1, [row_1]_\sim), (s_2, [row_2]_\sim)\big) \in \Xi$ iff (i) $\big((s_1, [row_1]_\sim), (s_2, [row_2]_\sim)\big) \in \Gamma^2$, (ii) $(s_1, s_2) \in E$, and (iii) $[row_1]_\sim \,{}^{=row_\varphi}\!\!\Rightarrow [row_2]_\sim$.

Note that the definition of Γ is well-given, since for all $row' \in [row]_\sim$, $row'[0] = row[0]$. The size of $G_{\varphi\sim\mathcal{K}}$ is bounded by $(|W| \cdot |\mathcal{R}ows^{\sim}_{\varphi}|)^2$.

Given a generic trace ρ of $\mathcal{K}$, we define the compass φ-structure *induced by* ρ as the fulfilling homogeneous compass φ-structure $\mathcal{G}_{(\mathcal{K},\rho)} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$, where $S = \{0, \ldots, |\rho|-1\}$, and for $0 \leq x < |\rho|$, $\mathcal{L}(x,x) \cap \mathcal{AP} = \mu(\rho(x))$ and $\mathcal{R}eq_D(\mathcal{L}(x,x)) = \emptyset$. Note that, given ρ, $\mathcal{G}_{(\mathcal{K},\rho)}$ always exists and is unique: all φ-atoms $\mathcal{L}(x,x)$ "on the diagonal" are determined by the labeling of $\rho(x)$ (and by the absence of requests). Moreover, by Lemma 17, all the other atoms $\mathcal{L}(x,y)$, for $0 \leq x < y < |\rho|$, are determined by the ${}^{=row_\varphi}\!\!\Rightarrow$ relation between φ-rows.

The following property can easily be proved by induction.

Proposition 33. *Given a Kripke structure* $\mathcal{K}$*, a trace* ρ *of* $\mathcal{K}$*, and a* $\mathrm{D}|_{\mathcal{H}om}$*-formula* φ*, for all* $0 \leq x \leq y < |\rho|$ *and for all subformulas* ψ *of* φ*:* $\mathcal{K}, \rho(x,y) \models \psi$ *iff* $\psi \in \mathcal{L}(x,y)$ *in* $\mathcal{G}_{(\mathcal{K},\rho)}$.

We can now introduce Theorem 34, that can be regarded as a version of Theorem 23 for MC.

Input: a Kripke structure $\mathcal{K} = (\mathcal{AP}, W, E, \mu, s_0)$, a D$|_{\mathcal{H}om}$-formula φ

1. Put $M \leftarrow |W| \cdot 2^{3|\varphi|^2}$, $step \leftarrow 0$ and $(s, row) \leftarrow (s_0, A)$ for some atom $A \in \mathcal{A}_\varphi$ with $\mathcal{R}eq_D(A) = \emptyset$ and $A \cap \mathcal{AP} = \mu(s_0)$.
2. If $\varphi \notin row[|row| - 1]$, return **yes**.
3. If $step = M - 1$, return **no**.
4. Non-deterministically choose s' such that $(s, s') \in E$.
5. Non-det. generate a φ-row row' and check that $row'[0] \cap \mathcal{AP} = \mu(s')$ and $row =^{row_\varphi}\!\!\Rightarrow row'$.
6. Put $step \leftarrow step + 1$ and $(s, row) \leftarrow (s', row')$.
7. Go back to 2.

Figure 6: Non-deterministic procedure deciding the existence of initial traces ρ such that $\mathcal{K}, \rho \not\models \varphi$

Theorem 34. *Given a Kripke structure $\mathcal{K} = (\mathcal{AP}, W, E, \mu, s_0)$ and a D$|_{\mathcal{H}om}$-formula φ, there exists an initial trace ρ of $\mathcal{K}$ such that $\mathcal{K}, \rho \models \varphi$ iff there exists a path in $G_{\varphi \sim \mathcal{K}} = (\Gamma, \Xi)$ from some node $(s_0, [row]_\sim) \in \Gamma$ to some node $(s, [row']_\sim) \in \Gamma$ such that: (1) there is $row_1 \in [row]_\sim$ with $|row_1| = 1$, and (2) there is $row_2 \in [row']_\sim$ with $\varphi \in row_2[|row_2| - 1]$.*

Proof. Preliminarily we observe that, in (1), if $|row_1| = 1$, then $\{row_1\} = [row]_\sim$; moreover, in (2), if for $row_2 \in [row']_\sim$ we have $\varphi \in row_2[|row_2| - 1]$, then for any $row_2' \in [row']_\sim$ we have $\varphi \in row_2'[|row_2'| - 1]$.

($\Rightarrow$) Let us consider an initial trace ρ such that $\mathcal{K}, \rho \models \varphi$, hence, by Proposition 33, $\varphi \in \mathcal{L}(0, |\rho| - 1)$ in the fulfilling homogeneous compass φ-structure induced by ρ, $\mathcal{G}_{(\mathcal{K},\rho)} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$. By Lemmata 15 and 17, $\mathcal{L}(0,0) =^{row_\varphi}\!\!\Rightarrow row_1 =^{row_\varphi}\!\!\Rightarrow \cdots =^{row_\varphi}\!\!\Rightarrow row_{|\rho|-1}$, and $\varphi \in row_{|\rho|-1}[|\rho| - 1]$. By definition of $(\varphi \sim \mathcal{K})$-graph, $(\rho(0), [\mathcal{L}(0,0)]_\sim) \xrightarrow{\Xi} (\rho(1), [row_1]_\sim) \xrightarrow{\Xi} \cdots \xrightarrow{\Xi} (\rho(|\rho| - 1), [row_{|\rho|-1}]_\sim)$ is a path in $\mathcal{G}_{(\mathcal{K},\rho)}$—since $row_y[0] \cap \mathcal{AP} = \mu(\rho(y))$ for all $0 \leq y < |\rho|$—satisfying requirements (1) and (2).

($\Leftarrow$) Let us assume there is a path $(s_0, [row_0]_\sim) \xrightarrow{\Xi} (s_1, [row_1]_\sim) \xrightarrow{\Xi} \cdots \xrightarrow{\Xi} (s_m, [row_m]_\sim)$ in the $(\varphi \sim \mathcal{K})$-graph $G_{\varphi \sim \mathcal{K}} = (\Gamma, \Xi)$, satisfying (1) and (2). Hence, by definition of $(\varphi \sim \mathcal{K})$-graph, $\rho = s_0 s_1 \cdots s_m$ is an (initial) trace of $\mathcal{K}$, $[row_0]_\sim =^{row_\varphi}\!\!\Rightarrow \cdots =^{row_\varphi}\!\!\Rightarrow [row_m]_\sim$, and $\mu(s_y) = row_y[0] \cap \mathcal{AP}$ for all $0 \leq y \leq m$. By applying repeatedly Lemma 21 we get that there exists a sequence $row_0' =^{row_\varphi}\!\!\Rightarrow \cdots =^{row_\varphi}\!\!\Rightarrow row_m'$ of φ-rows where $row_0' = row_0$, for every $0 \leq j \leq m$, $row_j' \in [row_j]_\sim$, and $\varphi \in row_m'[|row_m'| - 1]$. We observe that, by Definition 16, $|row_j'| = |row_{j-1}'| + 1$ for $1 \leq j \leq m$ and, since $|row_0'| = 1$, we have $|row_j'| = j + 1$. Let us now define $\mathcal{G} = (\mathbb{P}_\mathbb{S}, \mathcal{L})$ where $S = \{0, \ldots, m\}$ and $\mathcal{L}(x, y) = row_y'[y - x]$ for every $0 \leq x \leq y \leq m$. Note that $\mathcal{R}eq_D(\mathcal{L}(y, y)) = \emptyset$ for every $0 \leq y \leq m$ (by definition of φ-row). By Lemma 17, $\mathcal{G}$ is a fulfilling homogeneous compass φ-structure. Since $\mu(s_y) = row_y[0] \cap \mathcal{AP} (= \mathcal{L}(y, y) \cap \mathcal{AP})$ for all $0 \leq y \leq m$, then $\mathcal{G}$ is precisely the compass φ-structure induced by ρ. Finally, since $\varphi \in row_m'[m] = \mathcal{L}(0, m)$, by Proposition 33 we can conclude that $\mathcal{K}, \rho \models \varphi$. □

Now, analogously to the case of satisfiability, we can perform a reachability in $G_{\varphi \sim \mathcal{K}}$, exploiting the previous theorem to decide whether there is an initial trace ρ of $\mathcal{K}$ such that $\mathcal{K}, \rho \models \neg\varphi$, for a D$|_{\mathcal{H}om}$-formula φ (i.e., the complementary problem of MC $\mathcal{K} \models \varphi$). The *non-deterministic* procedure of Figure 6 searches for a suitable path in $G_{\varphi \sim \mathcal{K}}$, $(s_0, [row_0]_\sim) \xrightarrow{\Xi} \cdots \xrightarrow{\Xi} (s_m, [row_m]_\sim)$, where $row_0 = A \in \mathcal{A}_\varphi$ with $\mathcal{R}eq_D(A) = \emptyset$, $A \cap \mathcal{AP} = \mu(s_0)$, $m < M$, and $\neg\varphi \in row_m[|row_m| - 1]$ (i.e., $\varphi \notin row_m[|row_m| - 1]$). At the j-th iteration of lines 4./5., $(s_{j-1}, s_j) \in E$ is selected, and row_j is non-deterministically generated checking that $row_j[0] \cap \mathcal{AP} = \mu(s_j)$ and $row_{j-1} =^{row_\varphi}\!\!\Rightarrow row_j$.

Basically, the same observations about the working space of the procedure in Figure 4 can be done also for this algorithm, except for the space used to encode in binary $M \leq |W| \cdot 2^{3|\varphi|^2}$ and *step*, ranging in $[0, M-1]$, which is $O(\log |W| + |\varphi|^2)$ bits. Moreover we need to store two states, s and s' of $\mathcal{K}$, that need $O(\log |W|)$ bits to be represented.

Theorem 35. *The MC problem for* $\mathrm{D}|_{\mathcal{H}om}$*-formulas over finite Kripke structures is* ***PSPACE****-complete. Moreover, for constant-length formulas, it is* ***NLOGSPACE****-complete.*

Proof. Membership is immediate by the previous space analysis, and the fact that the complexity classes **NPSPACE** = **PSPACE** and **NLOGSPACE** are closed under complement.

As for the **PSPACE**-hardness, we make a reduction from the **PSPACE**-complete *problem of universality* of the language of an NFA [HK11]. The full proof is in Appendix A.2. For the **NLOGSPACE**-hardness, there exists a trivial reduction from the *problem of (non-)reachability* of two nodes in a directed graph. □

Finally, it is possible to adapt the procedure also for *strict* $\mathrm{D}|_{\mathcal{H}om}$ (using Definitions 25–27).

5 Conclusions

In this paper, we have shown that both satisfiability and model checking for the logic D of sub-intervals—over finite linear orders and finite Kripke structures, respectively—are **PSPACE**-complete, under the homogeneity assumption. We are investigating the possibility of generalizing the given procedures to cope with the logic BE: nothing is known about its satisfiability, while a large gap separates known upper and lower bounds for model checking.

Acknowledgements The work by Alberto Molinari, Angelo Montanari, and Pietro Sala has been supported by the GNCS project *Logic and Automata for Interval Model Checking*.

We sincerely thank an anonymous reviewer for his/her thorough review and valuable comments, which significantly contributed to improving the quality of the publication—in particular for spotting a problem with the hardness proof of satisfiability in the submitted paper, and suggesting a possible solution.

References

[All83] J. F. Allen. Maintaining knowledge about temporal intervals. *Communications of the ACM*, 26(11):832–843, 1983.

[BGMS09] D. Bresolin, V. Goranko, A. Montanari, and G. Sciavicco. Propositional interval neighborhood logics: Expressiveness, decidability, and undecidable extensions. *Annals of Pure and Applied Logic*, 161(3):289–304, 2009.

[BGMS10] D. Bresolin, V. Goranko, A. Montanari, and P. Sala. Tableaux for logics of subinterval structures over dense orderings. *Journal of Logic and Computation*, 20(1):133–166, 2010.

[BMM+16] L. Bozzelli, A. Molinari, A. Montanari, A. Peron, and P. Sala. Interval temporal logic model checking: The border between good and bad HS fragments. In *Proceedings of the 8th International Joint Conference (IJCAR)*, pages 389–405, 2016.

[DGMS11] D. Della Monica, V. Goranko, A. Montanari, and G. Sciavicco. Interval temporal logics: a journey. *Bulletin of the EATCS*, 105:73–99, 2011.

[HK11] M. Holzer and M. Kutrib. Descriptional and computational complexity of finite automata—a survey. *Information and Computation*, 209(3):456 – 470, 2011.

[HS91] J. Y. Halpern and Y. Shoham. A propositional modal logic of time intervals. *Journal of the ACM*, 38:279–292, 1991.

[KR93] H. Kamp and U. Reyle. *From Discourse to Logic: Introduction to Model-theoretic Semantics of Natural Language, Formal Logic and Discourse Representation Theory, Volume 42 of Studies in Linguistics and Philosophy.* Springer, 1993.

[Lod00] K. Lodaya. Sharpening the undecidability of interval temporal logic. In *Proceedings of the 6th Asian Computing Science Conference (ASIAN)*, pages 290–298, 2000.

[MM14] J. Marcinkowski and J. Michaliszyn. The undecidability of the logic of subintervals. *Fundamenta Informaticae*, 131(2):217–240, 2014.

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

[Mon16] A. Montanari. Interval temporal logics model checking. In *Proceedings of the 23rd International Symposium on Temporal Representation and Reasoning, (TIME)*, page 2, 2016.

[MPS10] A. Montanari, I. Pratt-Hartmann, and P. Sala. Decidability of the logics of the reflexive sub-interval and super-interval relations over finite linear orders. In *Proceedings of the 17th International Symposium on Temporal Representation and Reasoning (TIME)*, pages 27–34, 2010.

[Ott01] M. Otto. Two variable first-order logic over ordered domains. *Journal of Symbolic Logic*, 66(2):685–702, 2001.

[Sha04] I. Shapirovsky. On PSPACE-decidability in transitive modal logic. In *Proceedings of the 5th conference on Advances in Modal logic (AiML)*, pages 269–287, 2004.

[Ven90] Y. Venema. Expressiveness and completeness of an interval tense logic. *Notre Dame Journal of Formal Logic*, 31(4):529–547, 1990.

[Ven91] Y. Venema. A modal logic for chopping intervals. *Journal of Logic and Computation*, 1(4):453–476, 1991.

A Appendix

A.1 Proof of Lemma 21

Before we begin the proof, we introduce some extra notation and terminology. Given a φ-row row we denote by $row[i \dots j]$, for $0 \leq i \leq j < |row|$, the sub-word $row[i]row[i+1] \cdots row[j]$. Clearly any sub-word $row[0 \dots i]$ is a φ-row, for every $0 \leq i < |row|$; moreover, if $row =^{row_\varphi} \Rightarrow \overline{row}$, then $row[0 \dots i] =^{row_\varphi} \Rightarrow \overline{row}[0 \dots i+1]$. Given a φ-row $row = A_0^{m_0} \cdots A_n^{m_n}$, for every φ-atom A_i we say that A_i exceeds its rank in row if $m_i > rank(A_i)$. Finally we define a total order "$<$" on atoms $A_0, \dots, A_n$ determined by the position they have in row (i.e., $A_0 < \dots < A_n$). Note that "$<$" can be extended to (atoms of) pairs of φ-rows related by $\sim$.

We repeat the statement of Lemma 21 for convenience.

Lemma 21. Given two φ-row classes $[row_1]_\sim$ and $[row_2]_\sim$ such that $[row_1]_\sim =^{row_\varphi} \Rightarrow [row_2]_\sim$, *for every* $row \in [row_1]_\sim$ there exists $row' \in [row_2]_\sim$ such that $row =^{row_\varphi} \Rightarrow row'$.

Proof. Since $[row_1]_\sim =^{row_\varphi} \Rightarrow [row_2]_\sim$, there exists $row \in [row_1]_\sim$ and $\overline{row} \in [row_2]_\sim$ such that $row =^{row_\varphi} \Rightarrow \overline{row}$. If $|[row_1]_\sim| = 1$ the thesis follows. Let us now suppose $|[row_1]_\sim| \geq 2$; then there exists $row' \neq row$ such that $row' \sim row$. Let $row = A_0^{m_0} \cdots A_n^{m_n}$; by Definition, $row' = A_0^{m'_0} \cdots A_n^{m'_n}$, where for every $0 \leq i \leq n$, $m'_i = m_i$ if $m_i \leq rank(A_i)$, and $m'_i > rank(A_i)$ if $m_i > rank(A_i)$. Let $\overline{row} = \overline{A}_0^{\overline{m}_0} \cdots \overline{A}_{\overline{n}}^{\overline{m}_{\overline{n}}}$. The following algorithm generates $\overline{row}' = \overline{A}_0^{\overline{m}'_0} \cdots \overline{A}_{\overline{n}}^{\overline{m}'_{\overline{n}}}$ such that $row' =^{row_\varphi} \Rightarrow \overline{row}'$ and $\overline{row}' \sim \overline{row}$.

Algorithm A.1: BUILDSUCCESSOR$(row, \overline{row}, row')$

$i \leftarrow j \leftarrow 0$
$\overline{row}'[0] \leftarrow \overline{row}[0]$
$exit \leftarrow$ **false**
while $\neg exit$
- **if** $row[i] = row'[j]$
  - **then**
    - $\overline{row}'[j+1] \leftarrow \overline{row}[i+1]$
    - **if** $i < |row| - 1$ **then** $i \leftarrow i + 1$
    - **if** $j < |row| - 1$ **then** $j \leftarrow j + 1$ **else** $exit \leftarrow$ **true**
  - **else**
    - **if** $row[i] > row'[j]$ **then** $\overline{row}'[j+1] \leftarrow \overline{row}[i]$; $j \leftarrow j + 1$
    - **else** $i \leftarrow i + 1$ //$(row[i] < row'[j])$

return $\overline{row}'$

In order to prove that the returned φ-row $\overline{row}'$ satisfies the desired properties, we use the following invariant conditions, and show that they hold for every iteration of the while loop in the procedure:

(A) $row'[0 \dots j-1] =^{row_\varphi} \Rightarrow \overline{row}'$;

(B) $\overline{row}' \sim \overline{row}[0 \dots i]$
(note that in different iterations $\overline{row}'$ and $\overline{row}[0 \dots i]$ may change equivalence class);

(C) if $row[i] > row'[j]$ then $row[0 \dots i-1] \sim row'[0 \dots j]$ and the exponent of the atom $row'[j] = row[i-1]$ in $row'[0 \dots j]$ is greater than $rank(row[i-1]) = rank(row'[j])$;

(D) if $row[i] < row'[j]$ then $row[0 \dots i] \sim row'[0 \dots j-1]$ and the exponent of the atom $row[i] = row'[j-1]$ in $row[0 \dots i]$ is greater than $rank(row'[j-1]) = rank(row[i])$;

(E) if $row[i] = row'[j]$ then $row[0 \dots i] \sim row'[0 \dots j]$ and the two exponents of atoms $row[i]$ in $row[0 \dots i]$ and $row'[0 \dots j]$ are equal;

(G) if $row[i] < row'[j]$ then $row[i] = row[i-1]$.

Let us prove that the invariant conditions hold immediately before the execution of the while loop (i.e., before the first iteration of the while has taken place). Condition (A) trivially holds because $row'[0 \dots j-1]$ is the empty word, which is a predecessor of $\overline{row}'$ consisting of a single atom; moreover condition (E) is verified since $row[0 \dots i-1]$ is also the empty word. Condition (B) is verified because $\overline{row}' = \overline{row}[0]$. Conditions (C), (D) and (G) are vacuously verified because $i = j = 0$ and $row'[j] = row[i]$.

Let us now assume that, at the beginning of a generic iteration, the conditions (A)–(G) hold, and we prove that they hold after such iteration as well. The following cases may arise.

- $row[i] = row'[j]$. Then the algorithm puts $\overline{row}'[j+1] = \overline{row}[i+1]$. Since $\overline{row}' \sim \overline{row}[0 \dots i]$ by (B), we have that $\overline{row}'[j] = \overline{row}[i]$ (because j is the last position of $\overline{row}'$). Then, since $row =^{row_\varphi}\!\!\Rightarrow \overline{row}$, we have $row[i]\overline{row}[i] =^{D_\varphi}\!\!\Rightarrow \overline{row}[i+1]$ and thus $row'[j]\overline{row}'[j] =^{D_\varphi}\!\!\Rightarrow \overline{row}'[j+1]$, and since $row'[0 \dots j-1] =^{row_\varphi}\!\!\Rightarrow \overline{row}'[0 \dots j]$ by (A), we have $row'[0 \dots j] =^{row_\varphi}\!\!\Rightarrow \overline{row}'$: condition (A) is satisfied.

  Let us consider condition (B). If $\overline{row}[i+1] \neq \overline{row}[i]$ then the condition is trivially satisfied. Let us now consider the case $\overline{row}[i+1] = \overline{row}[i]$: by invariant condition (B) we have $\overline{row}'[0 \dots j] \sim \overline{row}[0 \dots i]$ and thus the exponents m and m' of the atoms $\overline{row}[i]$ and $\overline{row}'[j]$ in $\overline{row}[1 \dots i]$ and $\overline{row}[1 \dots j]$ satisfy either $m = m'$ or $m, m' > rank(\overline{row}[i])$. Since $\overline{row}[i+1] = \overline{row}[i]$ then $\overline{row}'[j+1] = \overline{row}'[j]$ and thus the invariant condition (B) is satisfied for $\overline{row}'$ and $\overline{row}[0 \dots i+1]$.

  Let us consider the conditions (C), (D), (E) and (G). Conditions (C), (D) and (G) hold trivially at the beginning of the current iteration since their preconditions are not satisfied, but one of them may hold non-trivially after the increment of indexes. In the case we are considering ($row[i] = row'[j]$) the following possibilities are given in the increment of i and j:

  - $i = |row| - 1$. Then, since $row[i] = row'[j]$, we have $row[i] = row'[j] = A_n$: two cases may arise. If $m_n = m'_n \leq rank(A_n)$, by invariant condition (E) we have $row[0 \dots i] \sim row'[0 \dots j]$ and thus $j = |row'| - 1$. At this point the procedure puts *exit* to true without incrementing neither i nor j and the invariant condition (E) is respected (invariant conditions (C), (D) and (G) are trivially respected because $row[i] = row'[j]$). Conversely, if $m_n, m'_n > rank(A_n)$ then, since invariant condition (E) holds, we have that $row[0 \dots i] \sim row'[0 \dots j]$; this means that the exponent m''_n of A_n in $row'[0 \dots j]$ satisfies $rank(A_n) < m''_n \leq m'_n$.[1] If $m''_n = m'_n$ the procedure terminates like in the previous case. If $m''_n < m'_n$, only j is incremented by 1, and the new exponent of A_n in $row'[0 \dots j+1]$ is $m''_n + 1 > rank(A_n)$. We have $row'[0 \dots j+1] \sim row[0 \dots i]$ and thus the invariant condition (E) is respected (invariant conditions (C), (D) and (G) are trivially respected because $row[i] = row'[j+1] = A_n$).

[1] Note: m''_n is the exponent of A_n in $row'[0 \dots j]$, whereas m'_n is the exponent of A_n in row'.

– $i < |row| - 1$. Then there exists the atom $row[0 \dots i+1]$. Two cases may arise: either $row'[j+1]$ exists or it does not. In the latter case $j = |row'| - 1$ and $row[i] = row'[j] = A_n$. Since $row[0 \dots i] \sim row'[0 \dots j]$, it cannot be the case that $m_n, m'_n \leq rank(A_n)$ because we will have that $m'_n \leq rank(A_n)$ and $m'_n < m_n \leq rank(A_n)$, violating $row \sim row'$. Thus $m_n, m'_n > rank(A_n)$. Since m'_n is the exponent of A_n in $row'[0 \dots j]$ ($row'[0 \dots j] = row'$) by invariant condition (E) we have that the exponent m''_n of A_n in $row[0 \dots i]$ satisfies $rank(A_n) < m''_n < m_n$ and thus the exponent $m''_n + 1$ of A_n in $row[0 \dots i+1]$ satisfies the same condition. Since in such situation the procedure increments only i and we just proved $row[0 \dots i+1] \sim row'[0 \dots j]$, then invariant (E) is preserved (invariant conditions (C), (D) and (G) are trivially respected because $row[i] = row'[j+1] = A_n$).

  Let us consider now the case in which $j < |row'| - 1$, and $row'[j+1]$ exists. Three cases may arise:

  * $row'[j+1] = row[i+1]$. Condition (E) is satisfied, and the premises of conditions (C), (D) and (G) are not fulfilled, hence they vacuously hold;
  * $row'[j+1] > row[i+1]$. Condition (D) is satisfied (we can reason as we did before for (E)) since $row'[j+1]$ is the first occurrence on row' of the atom $row'[j+1]$, while $row[i+1] = row[i]$ because row' and row feature the same atom. Hence also (G) is satisfied. The premises of both invariants (C) and (E) are not fulfilled, hence they vacuously hold;
  * $row'[j+1] < row[i+1]$. Condition (C) is satisfied (we can reason as we did before for (E)) since $row[i+1]$ is the first occurrence on row of the atom $row[i+1]$, while $row'[j+1] = row'[j]$ because row' and row feature the same atom. The premises of conditions (D), (E) and (G) are not fulfilled, hence they vacuously hold.

• $row[i] > row'[j]$. Then the algorithm puts $\overline{row}'[j+1] = \overline{row}[i]$. Let us prove that invariant condition (A) still holds for the updated $\overline{row}'$. By condition (C), $row[0 \dots i-1] \sim row'[0 \dots j]$ and the exponent of $row[i-1] = row'[j]$ in $row'[0 \dots j]$ is greater than $rank(row[i-1])$. Since the exponent of $row[i-1]$ in $row[0 \dots i]$ is equal to the exponent of $row[i-1]$ in row and it is greater than $rank(row[i-1])$ (as $row \sim row'$), then, by Lemma 18, there exists k such that $row[i-1-k]\overline{row}[i-1-k] =_{D_\varphi} \rightarrow \overline{row}[i-k]$ with $row[i-1-k] = row[i-1]$ and $\overline{row}[i-k] = \overline{row}[i-1-k]$, thus $row[i-1-k] = \dots = row[i-1]$ and $\overline{row}[i-k] = \overline{row}[i-k-1] = \dots = \overline{row}[i]$ (recall that $row =_{D_\varphi} \rightarrow \overline{row}$). By condition (B), $\overline{row}'[0 \dots j] \sim \overline{row}[0 \dots i]$, thus $\overline{row}'[j] = \overline{row}[i]$. Since $row'[j] = row[i-1]$ we have that $row'[j]\overline{row}'[j] =_{D_\varphi} \rightarrow \overline{row}[i] (= \overline{row}'[j+1])$ and thus condition (A) is verified.

  As for condition (B), first we prove that $\overline{row}[i]$ exceeds its rank in $\overline{row}$. Since, by condition (C), $row[i-1]$ exceeds its rank in row', and since $row' \sim row$, $row[i-1]$ exceeds its rank also in row. By Lemma 18, $\overline{row}[i]$ exceeds its rank in $\overline{row}$. By condition (B) we have $\overline{row}'[0 \dots i] \sim \overline{row}'[0 \dots j]$. Then the number of atoms $\overline{row}'[j]$ in $\overline{row}'[0 \dots j]$ exceeds its rank and thus, since $\overline{row}[i] = \overline{row}'[j] = \overline{row}'[j+1]$, condition (B) is respected for $\overline{row}'$.

  Now we consider the increment of j. Since we started from $row[i] > row'[j]$, then $row'[j+1]$ exists, as $row \sim row'$; we may have two cases:

  – $row[i] = row'[j+1]$. Then condition (E) is satisfied, as previously $row[0 \dots i-1] \sim row'[0 \dots j]$. Now there exists exactly one atom $row[i]$ in both. Conditions (C), (D), (G) trivially hold since their premises are not fulfilled;
  – $row[i] > row'[j+1]$. Since, by (C), $row[0 \dots i-1] \sim row'[0 \dots j]$ we have $row'[j+1] = row'[j] = row[i-1]$ and thus, previously, the exponent of $row'[j]$ exceeded its rank

in $row'[0 \dots j]$ (by (C)). Now, $row'[j+1]$ exceeds its rank in $row'[0 \dots j+1]$, hence condition (C) is satisfied. Invariant conditions (D), (E), (G) trivially hold since their premises are not fulfilled.

- $row[i] < row'[j]$. Then the algorithm just updates i to $i+1$. Condition (A) still holds since the value of j does not change.

  Let us consider condition (B). First we prove that $\overline{row}'[j]$ exceeds its rank in $\overline{row}'[0 \dots j]$: by condition (D), $row[i]$ exceeds its rank in $row[0 \dots i]$, and since $row[0 \dots i] \sim row'[0 \dots j-1]$, we have that $row'[j-1]$ exceeds its rank in $row'[0 \dots j-1]$; by Lemma 18 (recall that $row'[0 \dots j-1] =^{row}_{\varphi} \!\!\rightarrow \overline{row}'$) $\overline{row}'[j]$ exceeds its rank in $\overline{row}'[0 \dots j]$. Now we reason as follows. Since $row[i]$ exceeds its rank in $row[0 \dots i]$, by Lemma 18, $\overline{row}[i+1]$ exceeds its rank in $\overline{row}[0 \dots i+1]$. Moreover we already know, by (B), that $\overline{row}[0 \dots i] \sim \overline{row}'[0 \dots j]$, then $\overline{row}[i]$ exceeds its rank in $\overline{row}[0 \dots i]$. Now, if $\overline{row}[i+1] = \overline{row}[i]$, we conclude that $\overline{row}[0 \dots i+1] \sim \overline{row}'$, and thus condition (B) holds. To conclude we show that, in any case, if $\overline{row}[i+1] > \overline{row}[i]$, we get a contradiction.

  Let us assume that $\overline{row}[i+1] > \overline{row}[i]$, hence $\overline{row}[i+1]$ occurs just once in $\overline{row}[0 \dots i+1]$, thus its rank is 0, and it must be reflexive. If $\overline{row}[i]$ is irreflexive, its rank must be at least 1, hence it occurs at least two times (exceeding its rank in $\overline{row}[0 \dots i]$), and this is not possible. Thus $\overline{row}[i]$ is reflexive, hence $\mathcal{O}bs_D(\overline{row}[i]) \subseteq \mathcal{R}eq_D(\overline{row}[i])$. Moreover, by definition of $=^D_{\varphi}\!\!\rightarrow$, we have $\mathcal{R}eq_D(\overline{row}[i+1]) = \mathcal{R}eq_D(\overline{row}[i]) \cup \mathcal{O}bs_D(\overline{row}[i]) \cup \mathcal{R}eq_D(row[i]) \cup \mathcal{O}bs_D(row[i]) = \mathcal{R}eq_D(\overline{row}[i]) \cup \mathcal{R}eq_D(row[i]) \cup \mathcal{O}bs_D(row[i])$. As for $\overline{row}[i]$, $\mathcal{R}eq_D(\overline{row}[i]) = \mathcal{R}eq_D(\overline{row}[i-1]) \cup \mathcal{O}bs_D(\overline{row}[i-1]) \cup \mathcal{R}eq_D(row[i-1]) \cup \mathcal{O}bs_D(row[i-1])$. However, by (G) $row[i] = row[i-1]$, hence $\mathcal{R}eq_D(\overline{row}[i+1]) = \mathcal{R}eq_D(\overline{row}[i-1]) \cup \mathcal{O}bs_D(\overline{row}[i-1]) \cup \mathcal{R}eq_D(row[i-1]) \cup \mathcal{O}bs_D(row[i-1])$, which equals $\mathcal{R}eq_D(\overline{row}[i])$. Finally $\overline{row}[i] \cap \mathcal{AP} = \overline{row}[i-1] \cap row[i-1] \cap \mathcal{AP}$ and $\overline{row}[i+1] \cap \mathcal{AP} = \overline{row}[i] \cap row[i] \cap \mathcal{AP} = \overline{row}[i-1] \cap row[i-1] \cap \mathcal{AP}$. Thus, by Proposition 4, $\overline{row}[i] = \overline{row}[i+1]$, contradicting $\overline{row}[i+1] > \overline{row}[i]$.

  As for conditions (C)–(G) we have two possible cases (it cannot be that $row[i+1] > row'[j]$ because we started from $row[i] < row'[j]$):

  - $row[i+1] = row'[j]$. Condition (E) is satisfied since previously, by (D), $row[0 \dots i] \sim row'[0 \dots j-1]$, and now there exists exactly one atom $row[i+1]$ in both. Conditions (C), (D), (G) trivially hold since their premises are not fulfilled;
  - $row[i+1] < row'[j]$. Since by (D) $row[0 \dots i] \sim row'[0 \dots j-1]$, we have $row[i+1] = row[i] = row'[j-1]$ and thus, previously, the exponent of $row[i]$ exceeded its rank (D) in $row[0 \dots i]$; now $row[i+1]$ exceeds its rank in $row[0 \dots i+1]$. Thus invariant (D) is satisfied. Condition (G) is fulfilled as well. Conditions (E) and (C) trivially hold since their premises are not fulfilled.

At the end of the above procedure, the generated φ-row $\overline{row}'$ satisfies the desired properties, by invariant conditions (A) and (B). □

A.2 Hardness of MC for $\mathrm{D}|_{\mathcal{H}om}$ over finite Kripke structures

In this section we prove the **PSPACE**-hardness of MC for $\mathrm{D}|_{\mathcal{H}om}$ over finite Kripke structures by means of a reduction from the **PSPACE**-complete *problem of (non-)universality* of the language of a non-deterministic finite automaton [HK11]. We start by recalling some standard concepts.

A non-deterministic finite automaton (NFA) is a tuple $\mathcal{N} = (\Sigma, Q, q_1, \delta, F)$, where Σ is a finite alphabet, Q is a finite set of states, $q_1 \in Q$ is the *initial* state, $\delta : Q \times \Sigma \to 2^Q$ is the transition function, and $F \subseteq Q$ is the set of *accepting* states. Given a finite word w over Σ, with $|w| = n$, a

computation of $\mathcal{N}$ over w is a finite sequence of states $q'_1, \ldots, q'_{n+1}$ such that $q'_1 = q_1$, and for all $i \in [0, n-1]$, $q'_{i+2} \in \delta(q'_{i+1}, w(i))$. The language $\mathcal{L}(\mathcal{N})$ accepted by $\mathcal{N}$ consists of the finite words w over Σ such that there is a computation over w ending in some accepting state.

A deterministic finite automaton (DFA) is an NFA $\tilde{\mathcal{N}} = (\Sigma, \tilde{Q}, \tilde{q_1}, \tilde{\delta}, \tilde{F})$ such that for all $(q, c) \in \tilde{Q} \times \Sigma$, $\tilde{\delta}(q, c)$ is a singleton. It is well-known that, by a subset construction, we can build a DFA $\tilde{\mathcal{N}}$ from an NFA $\mathcal{N}$ such that $\mathcal{L}(\tilde{\mathcal{N}}) = \mathcal{L}(\mathcal{N})$ and $\tilde{Q} = 2^Q$.

The problem of deciding whether $\mathcal{L}(\mathcal{N}) \neq \emptyset$ for an NFA $\mathcal{N}$ can be solved by *logarithmic working space* by means of a non deterministic reachability from the initial state of $\mathcal{N}$ to an accepting state. On the other hand, deciding if $\mathcal{L}(\mathcal{N}) \neq \Sigma^*$ (namely, deciding if $\mathcal{L}(\mathcal{N})$ is *non-universal*, i.e., there is some $w \in \Sigma^*$ such that $w \notin \mathcal{L}(\mathcal{N})$) is more difficult, and it is **PSPACE**-complete [HK11]. This is due to the fact that the shortest word *not accepted* by an NFA can have length exponential in the number of states of the NFA.

In order to decide if a word w is accepted by an NFA $\mathcal{N}$, it is possible to build "on the fly" *the* computation of $\tilde{\mathcal{N}}$ (the DFA obtained by the aforementioned subset construction from $\mathcal{N}$, where $\mathcal{L}(\tilde{\mathcal{N}}) = \mathcal{L}(\mathcal{N})$) over w.

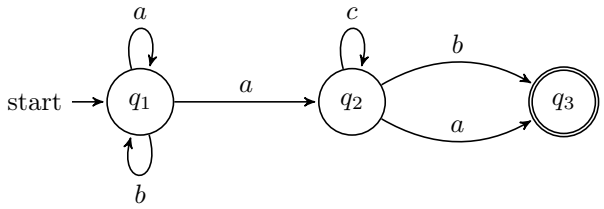

Figure 7: An example of NFA, where q_1 is the initial state, and q_3 the only final state.

For example, let us consider the NFA $\mathcal{N}$ of Figure 7. The computation of $\tilde{\mathcal{N}}$ (the equivalent DFA) over *aab* is:

$$(Q_1 = \{q_1\}) \xrightarrow{a} (Q_2 = \{q_1, q_2\}) \xrightarrow{a} (Q_3 = \{q_1, q_2, q_3\}) \xrightarrow{b} (Q_4 = \{q_1, q_3\}). \tag{1}$$

The word *aab* is accepted since there exists a final state of $\mathcal{N}$, $q_3 \in Q_4$ (Q_4 is the state of $\tilde{\mathcal{N}}$ reached by the computation). Note that Q_1 is the initial state of $\tilde{\mathcal{N}}$. The computation of $\tilde{\mathcal{N}}$ over *aac* is:

$$(Q_1 = \{q_1\}) \xrightarrow{a} (Q_2 = \{q_1, q_2\}) \xrightarrow{a} (Q_3 = \{q_1, q_2, q_3\}) \xrightarrow{c} (Q'_4 = \{q_2\}), \tag{2}$$

hence *aac* is *not* accepted since Q'_4 does not contain final states of $\mathcal{N}$.

Note that, as a rule, in the computation of $\tilde{\mathcal{N}}$ over w, with $|w| = n$,

$$Q_1 \xrightarrow{w(0)} Q_2 \xrightarrow{w(1)} \cdots \xrightarrow{w(n-2)} Q_n \xrightarrow{w(n-1)} Q_{n+1},$$

we have that the $\mathcal{N}$'s state $q \in Q_i$, for $0 \leq i \leq n$, *iff* there exists some computation of $\mathcal{N}$ over w,

$$q_1 \xrightarrow{w(0)} q_2 \xrightarrow{w(1)} \cdots \xrightarrow{w(n-2)} q_n \xrightarrow{w(n-1)} q_{n+1},$$

where $q = q_i$. Moreover, if some $q \in Q_i$ then all $q' \in \delta(q, w(i-1))$ must be in Q_{i+1} (we recall that δ is the transition function of the NFA $\mathcal{N}$). Conversely, if some $q' \in Q_{i+1}$ then it has to exist some $q \in Q_i$ such that $q' \in \delta(q, w(i-1))$.

We are now ready to reduce the **PSPACE**-complete problem of (non-)universality of the language of an NFA to the MC problem for $\mathrm{D}|_{\mathcal{H}om}$ over finite Kripke structures, proving that the latter is **PSPACE**-hard.

Given an NFA $\mathcal{N} = (\Sigma, Q, q_1, \delta, F)$, we build the Kripke structure $\mathcal{K}_\mathcal{N} = (\mathcal{AP}, W, E, \mu, s_0)$, where:

- $W = \{q_i^\top, q_i^\bot, q_i'^\top, q_i'^\bot \mid i = 1, \ldots, |Q|\} \cup \{x_1, x_2, v_1, v_2, v_1', v_2', \widehat{q_1}^\top, \widehat{q_2}^\bot, \ldots, \widehat{q_{|Q|}}^\bot\} \cup \Sigma$;
- $s_0 = v_1'$;
- $\mathcal{AP} = \{q_i, q_i' \mid i = 1, \ldots, |Q|\} \cup \Sigma \cup \{e_1, e_2, f_1, f_2\}$;
- $\mu(q_i{}^\top) = \mu(q_i'{}^\top) = \mathcal{AP}$, $\mu(q_i{}^\bot) = \mathcal{AP} \setminus \{q_i\}$, $\mu(q_i'{}^\bot) = \mathcal{AP} \setminus \{q_i'\}$, for $1 \le i \le |Q|$;
  $\mu(a) = \mathcal{AP} \setminus (\Sigma \setminus \{a\})$ for $a \in \Sigma$;
  $\mu(x_1) = \mathcal{AP} \setminus \{e_1\}$, $\mu(x_2) = \mathcal{AP} \setminus \{e_2\}$, $\mu(v_1) = \mu(v_1') = \mathcal{AP} \setminus \{f_1\}$, $\mu(v_2) = \mu(v_2') = \mathcal{AP} \setminus \{f_2\}$,
  and finally $\mu(\widehat{q_1}^\top) = \mathcal{AP}$, $\mu(\widehat{q_2}^\bot) = \mathcal{AP} \setminus \{q_2\}, \ldots, \mu(\widehat{q_{|Q|}}^\bot) = \mathcal{AP} \setminus \{q_{|Q|}\}$.

The edges E of $\mathcal{K}_\mathcal{N}$ can easily be deduced from Figure 8, which is an example of Kripke structure built for an NFA with set of states $Q = \{q_1, q_2, q_3\}$, and alphabet $\Sigma = \{a, b, c\}$.

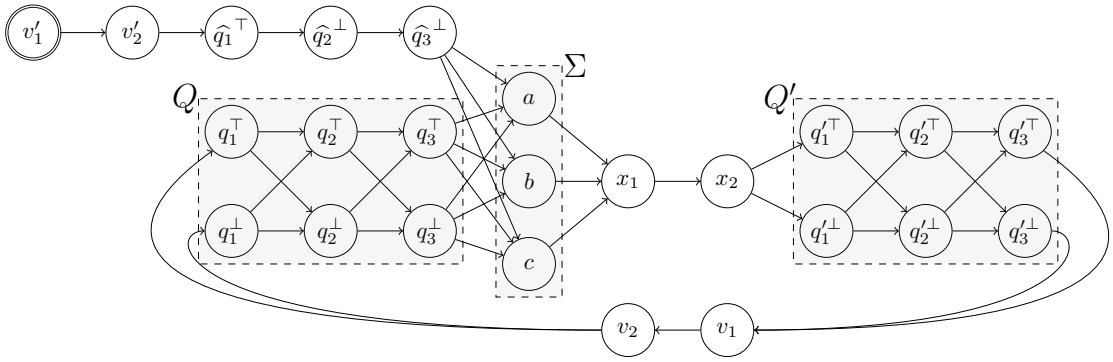

Figure 8: The Kripke structure $\mathcal{K}_\mathcal{N}$ built for an NFA with set of states $Q = \{q_1, q_2, q_3\}$ and alphabet $\Sigma = \{a, b, c\}$

The idea is that the computation of $\tilde{\mathcal{N}}$ on a word, say aab, which we have already seen in Equation 1, should be represented by the following initial trace of $\mathcal{K}_\mathcal{N}$:

$$
\begin{aligned}
&v_1'v_2'\underbrace{(\widehat{q_1}^\top \widehat{q_2}^\bot \widehat{q_3}^\bot)}_{Q_1} a x_1 x_2 \underbrace{(q_1'^\top q_2'^\top q_3'^\bot)}_{Q_2'} \cdots \\
&v_1 v_2 \underbrace{(q_1{}^\top q_2{}^\top q_3{}^\bot)}_{Q_2} a x_1 x_2 \underbrace{(q_1'^\top q_2'^\top q_3'^\top)}_{Q_3'} \cdots \\
&v_1 v_2 \underbrace{(q_1{}^\top q_2{}^\top q_3{}^\top)}_{Q_3} b x_1 x_2 \underbrace{(q_1'^\top q_2'^\bot q_3'^\top)}_{Q_4'} \cdots \\
&\qquad\qquad v_1 v_2 \underbrace{(q_1{}^\top q_2{}^\bot q_3{}^\top)}_{Q_4}.
\end{aligned}
\tag{3}
$$

The states $v_1, v_1', v_2, v_2', x_1, x_2$ are there only for technical reasons (explained later). A triple of states $(q_1{}^* q_2{}^* q_3{}^*)$ denoted by Q_i, where * stands for $\top$ or $\bot$, represents a state of $\tilde{\mathcal{N}}$, reached at the $(i-1)$-th step of the computation before reading $w(i-1)$: we have $q_j{}^\top$ if $q_j \in Q_i$, and $q_j{}^\bot$ if $q_j \notin Q_i$. Moreover the subtraces denoted by Q_i and Q_i' must be copies (i.e., $q_j{}^\top \in Q_i$ iff

${q'_j}^{\top} \in Q'_i$). In between Q_i and Q'_{i+1} in the trace we have $w(i-1) \in \Sigma$. The states $\widehat{q_1}^{\top}$, $\widehat{q_2}^{\perp}$ and $\widehat{q_3}^{\perp}$ of $\mathcal{K}_{\mathcal{N}}$ are just "copies" of ${q_1}^{\top}$, ${q_2}^{\perp}$ and ${q_3}^{\perp}$ respectively, added to ensure that the first state of the DFA $\tilde{\mathcal{N}}$ is $Q_1 = \{q_1\}$ (represented by $\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\widehat{q_3}^{\perp}$). Finally note that there is an intuitive match between subtraces and proposition letters satisfied. For example,

$$\mathcal{K}_{\mathcal{N}}, v_1 v_2 ({q_1}^{\top}{q_2}^{\top}{q_3}^{\top}) b x_1 x_2 ({q'_1}^{\top}{q'_2}^{\perp}{q'_3}^{\top}) \models (q_1 \wedge q_2 \wedge q_3) \wedge (q'_1 \wedge \neg q'_2 \wedge q'_3) \wedge (\neg a \wedge b \wedge \neg c).$$

Let us now come to the formula $\Phi_{\mathcal{N}}$, built from $\mathcal{N}$. We assume the *strict* semantic variant of $\mathrm{D}|_{\mathcal{H}om}$. Preliminarily, we define the following formulas, which exploit the auxiliary states $v_1, v'_1, v_2, v'_2, x_1, x_2$ in order to "select" some suitable traces:

$$\varphi_{trans} = \neg f_1 \wedge \neg f_2 \wedge [D](f_1 \wedge f_2) \wedge \langle D \rangle \top,$$

$$\varphi_{copy} = \neg e_2 \wedge \neg e_1 \wedge [D](e_1 \wedge e_2) \wedge \langle D \rangle \top.$$

We can prove that:

- $\mathcal{K}_{\mathcal{N}}, \rho \models \varphi_{trans}$ iff $\rho = \tilde{v_2} \cdots v_1$ and v_1, v_2 do not occur as internal states of ρ (where $\tilde{v_2}$ can be either v_2 or v'_2);
- $\mathcal{K}_{\mathcal{N}}, \rho \models \varphi_{copy}$ iff $\rho = x_2 \cdots x_1$ and x_1, x_2 do not occur as internal states of ρ.

Moreover the following formulas have an intuitive meaning (in particular $length_{\geq 3}$ is satisfied by a trace ρ iff $|\rho| \geq 3$):

$$\varphi_{reject} = \bigwedge_{q_i \in F} \neg q_i,$$

$$length_{\geq 3} = \langle D \rangle \top.$$

The formula $\Phi_{\mathcal{N}}$ is defined as follows (for the sake of brevity, for $q_i, q_j \in Q$ and $c \in \Sigma$ we denote $q_j \in \delta(q_i, c)$ as $(q_i, c, q_j) \in \delta$).

$$\Phi_{\mathcal{N}} := \underbrace{[D]\Big(\varphi_{trans} \rightarrow \Big(\Big(\bigwedge_{(q_i,a,q'_j)\in\delta} ((q_i \wedge a) \rightarrow q'_j)\Big) \wedge \Big(\bigwedge_{q'_i \in Q} (q'_i \rightarrow \bigvee_{(q_j,a,q'_i)\in\delta} (q_j \wedge a))\Big)\Big)\Big)}_{(1)} \wedge$$

$$\underbrace{[D](\varphi_{copy} \rightarrow \bigwedge_{q_i \in Q} (q_i \leftrightarrow q'_i))}_{(2)} \wedge \underbrace{\Big((e_1 \wedge length_{\geq 3} \wedge \varphi_{reject}) \vee \langle D \rangle \Big(\varphi_{copy} \wedge \varphi_{reject}\Big)\Big)}_{(3)}$$

Let us now prove the following lemma.

Lemma 36. *$\mathcal{L}(\mathcal{N}) \neq \Sigma^*$ iff there exists an initial trace ρ of $\mathcal{K}_{\mathcal{N}}$ such that $\mathcal{K}_{\mathcal{N}}, \rho \models \Phi_{\mathcal{N}}$.*

Proof. ($\Rightarrow$) If $\mathcal{L}(\mathcal{N}) \neq \Sigma^*$, then there is $w \notin \mathcal{L}(\mathcal{N})$. Therefore the computation of $\tilde{\mathcal{N}}$ over w is *not* accepting. Let us consider the initial trace ρ of $\mathcal{K}_{\mathcal{N}}$ encoding such a computation as explained before (see Equation 3). We distinguish two cases:

- $w = \varepsilon$: then we consider $\rho = v'_1 v'_2 \widehat{q_1}^{\top} \widehat{q_2}^{\perp} \cdots \widehat{q_{|Q|}}^{\perp}$. No strict subtrace satisfies φ_{trans} or φ_{copy}, hence conjuncts (1) and (2) are trivially satisfied. Moreover, since $\varepsilon \notin \mathcal{L}(\mathcal{N})$, $q_1 \notin F$, and thus ρ models also $e_1 \wedge length_{\geq 3} \wedge \varphi_{reject}$.

- $w \neq \varepsilon$; then we consider the initial trace ρ of $\mathcal{K}_{\mathcal{N}}$ encoding the computation over w, w.l.o.g. extended with some $c \in \Sigma$ (any symbol is fine), and finally x_1x_2: its generic form is $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}w(0)(x_1x_2{q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*v_1v_2{q_1}^*{q_2}^*\cdots{q_{|Q|}}^*c)^+x_1x_2$, where * is $^{\perp}$ or $^{\top}$, and $^+$ denotes a positive number of occurrences of the string in brackets. Every strict subtrace satisfying φ_{trans} models the right part of the implication in conjunct (1), which enforces the consistency conditions of a computation. Every strict subtrace satisfying φ_{copy} features ${q_i'}^{\top}$ if it features ${q_i}^{\top}$, and ${q_i'}^{\perp}$ if it features ${q_i}^{\perp}$, hence satisfies $\bigwedge_{q_i \in Q}(q_i \leftrightarrow q_i')$. Finally, the last part of ρ, $x_2{q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*v_1v_2{q_1}^*{q_2}^*\cdots{q_{|Q|}}^*cx_1$, models φ_{copy}, and, since w is *not* accepted, it also fulfills φ_{reject}.

Therefore, in both cases, there exists an initial trace ρ such that $\mathcal{K}_{\mathcal{N}}, \rho \models \Phi_{\mathcal{N}}$.

($\Leftarrow$) Let us assume there exists an initial trace ρ of $\mathcal{K}_{\mathcal{N}}$ such that $\mathcal{K}_{\mathcal{N}}, \rho \models \Phi_{\mathcal{N}}$. We distinguish some cases, according to the structure of ρ.

1. $\rho = v_1'(v_2')^?$ ($^?$ denotes 0 or 1 occurrences of the string in brackets).
   This trace does not model (3), thus it cannot be the trace we are looking for.

2. $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_j}^{\perp}$ for $j \geq 1$, or $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}c$ for some $c \in \Sigma$.
   No subtrace satisfies φ_{copy}, thus, by the conjunct (3), ρ models φ_{reject}. Hence $q_1 \notin F$, and ε is rejected by $\mathcal{N}$.

3. $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}cx_1(x_2)^?$
   This trace does not model the conjunct (3).

4. $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}cx_1x_2{q_1'}^*{q_2'}^*\cdots{q_j'}^*$ for $j \geq 1$
   This trace does not model the conjunct (3).

5. $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}cx_1x_2{q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*v_1(v_2)^?$
   This trace does not model the conjunct (3).

6. $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}cx_1x_2{q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*v_1v_2{q_1}^*{q_2}^*\cdots{q_j}^*$
   This trace does not model the conjunct (3).

7. $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}cx_1x_2{q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*v_1v_2{q_1}^*{q_2}^*\cdots{q_{|Q|}}^*c$
   This trace does not model the conjunct (3).

8. $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}cx_1x_2{q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*v_1v_2{q_1}^*{q_2}^*\cdots{q_{|Q|}}^*cx_1$
   This trace does not model the conjunct (3).

9. $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}c(x_1x_2{q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*v_1v_2{q_1}^*{q_2}^*\cdots{q_{|Q|}}^*c)^+x_1x_2$
   We have that, since ρ models the conjunct (1), *all* adjacent pairs of occurrences of ${q_1}^*{q_2}^*\cdots{q_{|Q|}}^* \rightsquigarrow {q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*$ consistently model a transition of $\tilde{\mathcal{N}}$; moreover *all* adjacent pairs of occurrences of ${q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^* \rightsquigarrow {q_1}^*{q_2}^*\cdots{q_{|Q|}}^*$ are "copies". Put all together, a legal computation of $\tilde{\mathcal{N}}$ over some string w is encoded. Finally, by the conjunct (3), a strict subtrace $x_2{q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*v_1v_2{q_1}^*{q_2}^*\cdots{q_{|Q|}}^*cx_1$ models φ_{reject}. Thus either w (if such subtrace is the last one) or one of its prefixes (if it is not the last one) is rejected by $\tilde{\mathcal{N}}$.

10. $\rho = v_1'v_2'\widehat{q_1}^{\top}\widehat{q_2}^{\perp}\cdots\widehat{q_{|Q|}}^{\perp}c(x_1x_2{q_1'}^*{q_2'}^*\cdots{q_{|Q|}'}^*v_1v_2{q_1}^*{q_2}^*\cdots{q_{|Q|}}^*c)^+x_1x_2\underline{{q_1'}^*{q_2'}^*\cdots{q_j'}^*}$.
    In this case and in the following ones, we underline the final part of ρ which may be "garbage", namely, it may encode an illegal suffix of a computation, just because it is not

forced to "behave correctly" by $\Phi_{\mathcal{N}}$. However, since the conjunct (3) is satisfied, a strict subtrace $x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2 {q_1}^* {q_2}^* \cdots {q_{|Q|}}^* c x_1$ models φ_{reject} (and this is not part of the garbage). Thus, as before, some word w or one of its prefixes is rejected by $\tilde{\mathcal{N}}$.

11. $\rho = v'_1 v'_2 \widehat{q_1}^\top \widehat{q_2}^\perp \cdots \widehat{q_{|Q|}}^\perp c(x_1 x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2 {q_1}^* {q_2}^* \cdots {q_{|Q|}}^* c)^+ x_1 x_2 \underline{{q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1}$.
Like the previous case.

12. $\rho = v'_1 v'_2 \widehat{q_1}^\top \widehat{q_2}^\perp \cdots \widehat{q_{|Q|}}^\perp c(x_1 x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2 {q_1}^* {q_2}^* \cdots {q_{|Q|}}^* c)^+ x_1 x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2$.
Like case 9, but a prefix of w is necessarily rejected, such that ρ encodes the computation of $\tilde{\mathcal{N}}$ over w.

13. $\rho = v'_1 v'_2 \widehat{q_1}^\top \widehat{q_2}^\perp \cdots \widehat{q_{|Q|}}^\perp c(x_1 x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2 {q_1}^* {q_2}^* \cdots {q_{|Q|}}^* c)^+ x_1 x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2 \underline{{q_1}^* {q_2}^* \cdots {q_j}^*}$,
$\rho = v'_1 v'_2 \widehat{q_1}^\top \widehat{q_2}^\perp \cdots \widehat{q_{|Q|}}^\perp c(x_1 x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2 {q_1}^* {q_2}^* \cdots {q_{|Q|}}^* c)^+ x_1 x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2 \underline{{q_1}^* {q_2}^* \cdots {q_{|Q|}}^* c}$,
$\rho = v'_1 v'_2 \widehat{q_1}^\top \widehat{q_2}^\perp \cdots \widehat{q_{|Q|}}^\perp c(x_1 x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2 {q_1}^* {q_2}^* \cdots {q_{|Q|}}^* c)^+ x_1 x_2 {q'_1}^* {q'_2}^* \cdots {q'_{|Q|}}^* v_1 v_2 \underline{{q_1}^* {q_2}^* \cdots {q_{|Q|}}^* c x_1}$.
All like case 12, just with the addition of final garbage, which is not considered, since it is not part of a strict subtrace satisfying φ_{copy}.

In all possible (legal) cases, we get that some string is rejected by $\tilde{\mathcal{N}}$ (and by $\mathcal{N}$). □

It follows that $\mathcal{L}(\mathcal{N}) = \Sigma^*$ iff $\mathcal{K}_{\mathcal{N}} \models \neg\Phi_{\mathcal{N}}$. Since also the *problem of universality* of the language of an NFA is **PSPACE**-complete (because **PSPACE** is closed under complement), and both $\mathcal{K}_{\mathcal{N}}$ and $\Phi_{\mathcal{N}}$ can be generated in polynomial time, we have proved the following.

Theorem 37. *The MC problem for* $\mathrm{D}|_{\mathcal{H}om}$*-formulas over finite Kripke structures is* ***PSPACE****-hard.*

Finally, by slightly modifying $\Phi_{\mathcal{N}}$, we can adapt the proof to the *proper* semantic variant of $\mathrm{D}|_{\mathcal{H}om}$.

A.3 Hardness of satisfiability for $\mathrm{D}|_{\mathcal{H}om}$ over finite linear orders

In this section we outline a **PSPACE**-hardness proof for the satisfiability problem for $\mathrm{D}|_{\mathcal{H}om}$-formulas over finite linear orders.

The construction mimics that of Sections 3.2 and 3.3 of [MM14], in which the authors show that it is possible to build a formula Ψ of D which encodes accepting computations of an NFA. More precisely the set of letters of Ψ equals the union of the alphabet of the NFA and the set of its states (plus some auxiliary letters, to enforce the "orientation" in the linear order, something that D is unaware of), and Ψ is satisfied by all and only the models such that the point-intervals are labeled with an accepting computation of the NFA over the word written in its point-intervals.

The idea is then to exploit Ψ to encode the Kripke structure of the previous section, thus getting a reduction from the problem of non-universality of the language of an NFA to the satisfiability problem for $\mathrm{D}|_{\mathcal{H}om}$. As a matter of fact, a Kripke structure can be regarded as a trivial NFA over a unary alphabet, say $\{a\}$, such that all the states are final, as we are interested only in the structure of traces (i.e., any word/trace is accepted under the only constraint that it exists in the structure).

By an easy adaptation of the results of Sections 3.2 and 3.3 of [MM14] we get the following.

Proposition 38. *Given a Kripke structure* $\mathcal{K} = (\mathcal{AP}, W, E, \mu, s_0)$ *devoid of self-loops, there exists a* $\mathrm{D}|_{\mathcal{H}om}$*-formula* $\Psi_{\mathcal{K}}$ *whose set of proposition letters is* $\mathcal{AP} \cup W \cup Aux$*—being Aux a set of auxiliary letters—such that any finite linear order satisfying* $\Psi_{\mathcal{K}}$ *represents an initial trace of* $\mathcal{K}$*. Moreover* $\Psi_{\mathcal{K}}$ *is polynomial in the size of* $\mathcal{K}$*.*

Every linear order satisfying $\Psi_{\mathcal{K}}$ features states of $\mathcal{K}$ labeling point-intervals (exactly one state for each point). Moreover we can easily force, for each occurrence of some state s of $\mathcal{K}$ along the order, the set of letters $\mu(s)$ to hold on the same position (point). The structure $\mathcal{K}$ in Proposition 38 must not feature self-loops for a technical reason: by fulfilling this requirement, there is no way for a state of $\mathcal{K}$ to "span" (by homogeneity) more than one point in a linear order satisfying $\Psi_{\mathcal{K}}$. We observe that in [MM14] the authors do not assume homogeneity; however homogeneity does not cause problems in our construction, as, intuitively, all the significant properties stated by $\Psi_{\mathcal{K}}$ are related to point-intervals.

Let us observe that the Kripke structure of the previous section does not contain self-loops. By Lemma 36, the language of an NFA $\mathcal{N}$ is non-universal iff there exists an initial trace ρ such that $\mathcal{K}_{\mathcal{N}}, \rho \models \Phi_{\mathcal{N}}$ (the Kripke structure and formula built from $\mathcal{N}$ in the previous section), iff (by Proposition 38 applied to $\mathcal{K}_{\mathcal{N}}$) the formula $\Psi_{\mathcal{K}_{\mathcal{N}}} \wedge \Phi_{\mathcal{N}}$ is satisfiable. We have proved the next theorem.

Theorem 39. *The satisfiability problem for* $\mathrm{D}|_{\mathcal{H}om}$*-formulas over finite linear orders is* ***PSPACE****-hard.*