Decidability of Iteration-free PDL with Parallel Composition

Philippe Balbiani and Joseph Boudou *

Institut de recherche en informatique de Toulouse, Université de Toulouse
Joseph.Boudou@irit.fr, Philippe.Balbiani@irit.fr

Abstract. PRSPDL is a highly undecidable propositional dynamic logic with an operator for parallel composition of programs. This operator has a separation semantic such that a multiplicative conjunction similar to the one found in the logic of Boolean bunched implications is definable. The present work identifies an iteration-free decidable fragment of PRSPDL in which the multiplicative conjunction is still definable. A NEXPTIME complexity upper bound for the fragment is given.

1 Introduction

The propositional dynamic logic (PDL) is a multi-modal logic designed for reasoning about the behaviour of programs [7, 10, 9]. With each program α is associated the modal operator $[\alpha]$, formulas $[\alpha]\varphi$ being read "all executions of α from the current state lead to a state where φ holds". The set of modal operators is inductively extended by some compound constructs: composition $(\alpha\ ;\ \beta)$ of programs α and β corresponds to the composition of the accessibility relations $R(\alpha)$ and $R(\beta)$; test $\varphi?$ on formula ϕ corresponds to the partial identity relation in the subsets of the Kripke models in which the formula φ is true; iteration $\alpha^\star$ corresponds to the reflexive and transitive closure of $R(\alpha)$. The problem with PDL is that the states of the Kripke models in which formulas are evaluated have no internal structure.

The logics of Boolean bunched implications (BBI) extend the classical propositional logic by adding a multiplicative intuitionistic conjunction operator $*$, formulas $(\varphi * \psi)$ being read "the current state can be split into two states respectively satisfying φ and ψ" and a multiplicative intuitionistic implication operator $-\!\!*$, formulas $(\varphi -\!\!* \psi)$ being read "if the current state is combined with a state satisfying φ, then the resulting state satisfies ψ" [15]. This logic can be viewed as a modal logic with two related binary modalities. In the corresponding Kripke semantic, frames have a ternary relation $\lhd$, $x \lhd (y, z)$ denoting both that x can be split into y and z and that y and z can be combined to produce x. BBI is semidecidable [8, 12] and undecidable [13, 6]. It forms the base ground for separations logics [16], some of them being decidable. One of the most significant

* This work was supported by the "French National Research Agency" (DynRes contract ANR-11-BS02-011).

application of separation logics, proposed by O'Hearn and Brookes [14, 5], consists in a Hoare-style logic for the verification of concurent programs with shared ressources. It would be interesting to have a dynamic logic related to O'Hearn and Brookes's logic as PDL is related to Hoare's logic.

The propositional dynamic logic with storing, recovering and parallel composition (PRSPDL), introduced by Benevides and al. [3], extends the syntax of PDL by adding the storing programs s_1 and s_2, the recovering programs r_1 and r_2, and the parallel composition of programs binary operator $\|$. In the corresponding Kripke semantic, all these new constructs are interpreted by means of a ternary operator $\lhd$ playing the same role as in BBI's Kripke semantic. Whenever $x \lhd (y, z)$, y is related to x by s_1, z is related to x by s_2 and x is related to y and z by respectively r_1 and r_2. The parallel composition $(\alpha \parallel \beta)$ corresponds to the fork $R(\alpha)\nabla R(\beta)$ of $R(\alpha)$ and $R(\beta)$ defined as follows: whenever $w_1 \lhd (w_2, w_3)$, $w_6 \lhd (w_4, w_5)$, w_2 and w_4 are related by $R(\alpha)$ and w_3 and w_5 by $R(\beta)$, then w_1 and w_6 are related by $R(\alpha)\nabla R(\beta)$. A multiplicative conjonction similar to the one found in separation logics can be defined in PRSPDL by $(\varphi * \psi) \doteq \langle \varphi? \parallel \psi? \rangle \top$. Hence this logic is both a dynamic logic and a separation logic. Unfortunately, PRSPDL has been proved to be highly undecidable [2].

The purpose of this paper is to present a decidable fragment of PRSPDL in which the multiplicative conjunction is still definable. More precisely, we prove that the satisfiability problem for this fragment is in NEXPTIME. The method used is the classical selection of a finite model [4]. The main difficulty is that no comprehensive set of subformulas can be expressed in the langage for a formula of the form $[\alpha \parallel \beta]\varphi$. This difficulty is overcome by adding placeholders on the syntactic side and markers on the semantic side.

The next section presents the language and the semantic of the studied fragment. Section 3 adapts the usual unfolding model operation [4] to the studied frame. Section 4 presents the placeholders and markers. Section 5 proves decidabilty of the fragment, giving a complexity upper bound.

2 Language and Semantic

We consider the fragment $\mathrm{PPDL}_0^{\mathrm{det}}$ of PRSPDL without program iterations and the special programs r_1, r_2, s_1, s_2. This corresponds to the iteration-free PDL language with sequential compositions, tests and parallel compositions. Formaly, the language of $\mathrm{PPDL}_0^{\mathrm{det}}$ is defined as follows.

Let Φ_0 be a set of propositional variables and Π_0 a countable set of atomic program variables. The sets Φ and Π of formulas and programs are languages over the alphabet of symbols $\Phi_0 \cup \Pi_0 \cup \{;, ?, \|, \bot, [,], (,)\}$ defined by:

$$\alpha, \beta := a \mid (\alpha \,;\, \beta) \mid \phi? \mid (\alpha \parallel \beta)$$
$$\varphi := p \mid \bot \mid [\alpha]\varphi$$

where p range over Φ_0, a over Π_0, φ over Φ and α and β over Π.

The usual common operators like implication and diamond can easily be defined, respectively by $\varphi \to \psi \doteq [\varphi?]\,\psi$ and $\langle \alpha \rangle\, \varphi \doteq [[\alpha \,;\, \varphi?]\, \bot?]\, \bot$. Moreover,

the multiplicative conjunction related to BBI may be defined by $\varphi * \psi \doteq [[\varphi? \parallel \psi?]\bot?]\bot$. Althought these operators may be usefull in applications, they are not needed here and for the sake of simplicity, they will not be used in the remaining of the paper.

A model is a tuple $\mathcal{M} = (W, R, \lhd, V)$ where W is a non-empty set of worlds, $R : \Pi_0 \longrightarrow \mathcal{P}\left(W^2\right)$ is a function from atomic programs to corresponding accessibility relations, $\lhd \subseteq W^3$ is the separation relation and $V : \Phi_0 \longrightarrow \mathcal{P}(W)$ is the valuation function. The language Φ is interpreted over $\lhd$-separated $\lhd$-deterministic models, i.e. models such that $\forall w, w_1, w_2, v, v_1, v_2 \in W$:

$$w \lhd (w_1, w_2) \wedge w \lhd (v_1, v_2) \Rightarrow w_1 = v_1 \wedge w_2 = v_2 \qquad (\lhd\text{-separated})$$
$$w \lhd (w_1, w_2) \wedge v \lhd (w_1, w_2) \Rightarrow w = v \qquad (\lhd\text{-deterministic})$$

The forcing relation $\vDash$ is defined by parallel induction along with the extension of R to all programs:

$$\begin{array}{ll}
\mathcal{M}, w \vDash p & \text{iff } w \in V(p) \\
\mathcal{M}, w \vDash \bot & \text{never} \\
\mathcal{M}, w \vDash [\alpha]\varphi & \text{iff } \forall w',\ wR(\alpha)w' \Rightarrow \mathcal{M}, w' \vDash \varphi \\
w\ R(\alpha\ ;\ \beta)\ w' & \text{iff } \exists w'',\ wR(\alpha)w'' \wedge w''R(\beta)w' \\
w\ R(\varphi?)\ w' & \text{iff } w = w' \wedge \mathcal{M}, w \vDash \varphi \\
w\ R(\alpha \parallel \beta)\ w' & \text{iff } \exists w_1, w_2, w_3, w_4, \\
 & \qquad w \lhd (w_1, w_2) \wedge w_1 R(\alpha) w_3 \wedge w_2 R(\beta) w_4 \wedge w' \lhd (w_3, w_4)
\end{array}$$

As usual, a formula $\varphi \in \Phi$ is said to be *satisfiable* iff there exists a model $\mathcal{M}$ and a world w such that $\mathcal{M}, w \vDash \varphi$.

In order to ease inductive reasoning about this logic, the length of both formulas and programs is defined.

Definition 1 (Length). *The lengths $|\varphi| \in \mathbb{N}$ and $|\alpha| \in \mathbb{N}$ of each formula $\varphi \in \Phi$ and each program $\alpha \in \Pi$ is inductively defined as:*

$$\begin{array}{cc}
|p| = 0 & |a| = 1 \\
|\bot| = 0 & |\alpha\ ;\ \beta| = |\alpha| + |\beta| + 1 \\
|[\alpha]\varphi| = |\alpha| + |\varphi| & |\varphi?| = |\varphi| + 1 \\
 & |\alpha \parallel \beta| = |\alpha| + |\beta| + 1
\end{array}$$

Lemma 1. *The length of any formula $\varphi \in \Phi$ is bounded by the number of occurences of symbols in φ.*

Proof. We prove simultaneously the corresponding property for programs: the length of any program $\alpha \in \Pi$ is bounded by the number of occurences of symbols in α. The proof is by parallel induction on the number of occurences of symbols in φ and α respectively and is left to the reader. □

Definition 2 (Size). *The size* $\mathrm{size}(\alpha)$ *of any program* $\alpha \in \Pi$ *is inductively defined as:*

$$\begin{aligned}\mathrm{size}(a) &= 1\\ \mathrm{size}(\varphi?) &= 0\\ \mathrm{size}(\alpha\,;\beta) &= \mathrm{size}\,\alpha + \mathrm{size}\,\beta\\ \mathrm{size}(\alpha \parallel \beta) &= \mathrm{size}\,\alpha + \mathrm{size}\,\beta\end{aligned}$$

Lemma 2. *For all* $\alpha \in \Pi$, $\mathrm{size}(\alpha) \leq |\alpha|$.

Proof. By induction on the number of occurences of symbols in α, left to the reader. □

Lemma 3. *Given any* $\lhd$*-deterministic model* $\mathcal{M} = (W, R, \lhd, V)$*, for all* $\alpha \in \Pi$ *and* $w, v \in W$*, if* $wR(\alpha)v$ *and* $\mathrm{size}(\alpha) = 0$*, then* $w = v$.

Proof. By induction on the length of α. The cases for atomic programs and tests are trivial. For sequential composition, the property holds by induction. Let suppose $wR(\alpha \parallel \beta)v$ and $\mathrm{size}(\alpha \parallel \beta) = 0$. Then there exists $w_1, w_2, w_3, w_4 \in W$ such that $w \lhd (w_1, w_2)$, $w_1R(\alpha)w_3$, $w_2R(\beta)w_4$ and $v \lhd (w_3, w_4)$. By induction, $w_1 = w_3$ and $w_2 = w_4$. Since $\mathcal{M}$ is $\lhd$-deterministic, $w = v$. □

3 Model Unfolding

Definition 3 (Bounded morphism). *Given two* $\lhd$*-separated* $\lhd$*-deterministic models* $\mathcal{M} = (W, R, \lhd, V)$ *and* $\mathcal{M}' = (W', R', \lhd', V')$*, a mapping* $f : \mathcal{M} \longrightarrow \mathcal{M}'$ *is called* a bounded morphism *iff it satisfies the following conditions for all* $v, w, w_1, w_2 \in W$*,* $w', w'_1, w'_2 \in W'$ *and* $a \in \Pi_0$*:*

$$w \text{ and } f(w) \text{ satisfy the same propositional variables} \tag{1}$$

$$vR(a)w \Rightarrow f(v)R'(a)f(w) \tag{2}$$

$$f(v)R'(a)w' \Rightarrow \exists w,\ f(w) = w' \text{ and } vR(a)w \tag{3}$$

$$w \lhd (w_1, w_2) \Rightarrow f(w) \lhd' (f(w_1), f(w_2)) \tag{4}$$

$$f(w) \lhd' (w'_1, w'_2) \Rightarrow \exists w_1, w_2, f(w_1) = w'_1, f(w_2) = w'_2 \text{ and } w \lhd (w_1, w_2) \tag{5}$$

$$w' \lhd' (f(w_1), f(w_2)) \Rightarrow \exists w,\ f(w) = w' \text{ and } w \lhd (w_1, w_2) \tag{6}$$

Proposition 1. *If* f *is a bounded morphism from* $\mathcal{M}$ *to* $\mathcal{M}'$*, then for all* $w \in W$ *and* $\varphi \in \Phi$*,* $\mathcal{M}, w \vDash \varphi$ *iff* $\mathcal{M}', f(w) \vDash \varphi$.

Proof. By simultaneous induction on the length of both $\varphi \in \Phi$ and $\alpha \in \Pi$, the following properties can be proved:

$$\begin{aligned}\mathcal{M}, w \vDash \varphi &\Leftrightarrow \mathcal{M}', f(w) \vDash \varphi\\ vR(\alpha)w &\Rightarrow f(v)R'(\alpha)f(w)\\ f(v)R'(\alpha)w' &\Rightarrow \exists w,\ f(w) = w' \text{ and } vR(\alpha)w\end{aligned}$$

□

Given a $\lhd$-separated $\lhd$-deterministic countable model $\mathcal{M}' = (W', R', \lhd', V')$ and a world $w'_0 \in W'$, we will construct the *unfolding* of $\mathcal{M}'$ at w'_0 as follows. Let W_∞ be a countably infinite set. For all $k \in \mathbb{N}$ we will construct the tuple $T_k = (W_k, R_k, \lhd_k, h_k, d_k, p_k)$ such that $W_k \subseteq W_\infty$, $\mathcal{M}_k = (W_k, R_k, \lhd_k, V_k)$ is a model, $h_k : W_k \longrightarrow W'$ is a function satisfying the conditions (2) and (4) of Definition 3, $d_k : W_k \longrightarrow \mathbb{Q}$ gives the *degree* of worlds in W_k and $p_k : W_k \longrightarrow \mathbb{Z}$ gives the *depth* of worlds in W_k.

We define the following defects:

1. A tuple $(v, a, w') \in W_\infty \times \Pi_0 \times W'$ is a defect of type 1 for T_k iff $v \in W_k$, $h_k(v)R'(a)w'$ and $\forall w \in W_k$, $h_k(w) = w'$ implies $(v, w) \notin R_k(a)$;
2. A tuple $(v, w'_1, w'_2) \in W_\infty \times W' \times W'$ is a defect of type 2 for T_k iff $v \in W_k$, $h_k(v) \lhd' (w'_1, w'_2)$ and $\forall w_1, w_2 \in W_k$, $h_k(w_1) = w'_1 \wedge h_k(w_2) = w'_2$ implies $(v, w_1, w_2) \notin \lhd_k$;
3. A tuple $(w', w_1, w_2) \in W' \times W_\infty \times W_\infty$ is a defect of type 3 for T_k iff $w_1, w_2 \in W_k$, $w' \lhd' (h_k(w_1), h_k(w_2))$ and $\forall w \in W_k$, $h_k(w) = w'$ implies $(w, w_1, w_2) \notin \lhd_k$.

As all sets W_∞, W' and Π_0 are countable, there exists an enumeration $\delta_0, \delta_1 \ldots$ of tuples belonging to $(W_\infty \times \Pi_0 \times W') \cup (W_\infty \times W' \times W') \cup (W' \times W_\infty \times W_\infty)$ where each tuple appears infinitely often.

As a first step, let $w_0 \in W_\infty$, $W_0 = \{w_0\}$, $R_0(a) = \emptyset$ for all $a \in \Pi_0$, $\lhd_0 = \emptyset$, $h_0(w_0) = w'_0$, $d_0(w_0) = 0$ and $p_0(w_0) = 0$.

Next, given the k-tuple T_k, if δ_k is not a defect for T_k then $T_{k+1} = T_k$. Otherwise, depending on the type of δ_k one of the following rule is applied.

1. When δ_k is of type 1, let $\delta_k = (v, a, w')$ and w^+ be a fresh element from W_∞

$$\begin{aligned} W_{k+1} &= W_k \cup \{w^+\} \\ R_{k+1}(a) &= R_k(a) \cup \{(v, w^+)\} \\ R_{k+1}(b) &= R_k(b) \text{ for all } b \neq a \\ \lhd_{k+1} &= \lhd_k \end{aligned} \qquad \begin{aligned} h_{k+1}(w) &= \begin{cases} w' & \text{if } w = w^+ \\ h_k(w) & \text{otherwise} \end{cases} \\ d_{k+1}(w) &= \begin{cases} d_k(v) + 1 & \text{if } w = w^+ \\ d_k(w) & \text{otherwise} \end{cases} \\ p_{k+1}(w) &= \begin{cases} p_k(v) & \text{if } w = w^+ \\ p_k(w) & \text{otherwise} \end{cases} \end{aligned}$$

2. When δ_k is of type 2, let $\delta_k = (v, w'_1, w'_2)$ and w_1^+ and w_2^+ be fresh elements from W_∞

$$\begin{aligned} W_{k+1} &= W_k \cup \{w_1^+, w_2^+\} \\ R_{k+1}(a) &= R_k(a) \text{ for all } a \\ \lhd_{k+1} &= \lhd_k \cup \{(v, w_1^+, w_2^+)\} \end{aligned} \qquad \begin{aligned} h_{k+1}(w) &= \begin{cases} w'_1 & \text{if } w = w_1^+ \\ w'_2 & \text{if } w = w_2^+ \\ h_k(w) & \text{otherwise} \end{cases} \\ d_{k+1}(w) &= \begin{cases} \frac{1}{2} d_k(v) & \text{if } w \in \{w_1^+, w_2^+\} \\ d_k(w) & \text{otherwise} \end{cases} \\ p_{k+1}(w) &= \begin{cases} p_k(v) + 1 & \text{if } w \in \{w_1^+, w_2^+\} \\ p_k(w) & \text{otherwise} \end{cases} \end{aligned}$$

3. When δ_k is of type 3, let $\delta_k = (w', w_1, w_2)$ and w^+ be a fresh element from W_∞

$$W_{k+1} = W_k \cup \{w^+\} \qquad h_{k+1}(w) = \begin{cases} w' & \text{if } w = w^+ \\ h_k(w) & \text{otherwise} \end{cases}$$
$$R_{k+1}(a) = R_k(a) \text{ for all } a$$
$$\lhd_{k+1} = \lhd_k \cup \{(w^+, w_1, w_2)\} \qquad d_{k+1}(w) = \begin{cases} d_k(w_1) + d_k(w_2) & \text{if } w = w^+ \\ d_k(w) & \text{otherwise} \end{cases}$$
$$p_{k+1}(w) = \begin{cases} p_k(w_1) - 1 & \text{if } w = w^+ \text{ and } p_k(w_1) = p_k(w_2) \\ -1 & \text{if } w = w^+ \text{ and } p_k(w_1) \neq p_k(w_2) \\ p_k(w) & \text{otherwise} \end{cases}$$

Then let W, R and $\lhd$ be the union of respectively W_k, R_k and $\lhd_k$ on all $k \in \mathbb{N}$. We further define the functions $h(w) = h_{k_w}(w)$, $d(w) = d_{k_w}(w)$ and $p(w) = p_{k_w}(w)$ for all $w \in W$, k_w being the smallest k such that $w \in W_k$. Finaly, let $V(p) = \{w \in W \mid h(w) \in V'(p)\}$ for all $p \in \Phi_0$. The model $\mathcal{M} = (W, R, \lhd, V)$ is the *unfolding* of $\mathcal{M}'$ at w'_0. The initial world w_0 is called the *root* of the unfolding.

Lemma 4. *For all $w, v, w_1, w_2 \in W$, $k \in \mathbb{N}$, $a \in \Pi_0$, $w' \in W'$, $r \in \mathbb{Q}$ and $z \in \mathbb{Z}$, the following implications hold:*

$$w \in W_k \Rightarrow w \in W_{k+1} \tag{7}$$
$$vR_k(a)w \Rightarrow vR_{k+1}(a)w \tag{8}$$
$$w \lhd_k (w_1, w_2) \Rightarrow w \lhd_{k+1} (w_1, w_2) \tag{9}$$
$$h_k(w) = w' \Rightarrow h_{k+1}(w) = w' \tag{10}$$
$$d_k(w) = r \Rightarrow d_{k+1}(w) = r \tag{11}$$
$$p_k(w) = z \Rightarrow p_{k+1}(w) = z \tag{12}$$

Proof. Each implication is easily checked for each type of the defect δ_k. □

Lemma 5. *The model $\mathcal{M}$ is $\lhd$-separated and $\lhd$-deterministic.*

Proof. It suffices to check that for all $k \in \mathbb{N}$, the model $(W_k, R_k, \lhd_k, V\restriction_{W_k})$ is $\lhd$-separated and $\lhd$-deterministic, which is left to the reader. □

Lemma 6. *The map h is a bounded morphism from $\mathcal{M}$ to $\mathcal{M}'$.*

Proof. Condition (1) holds by definition of V. The fact that for all $k \in \mathbb{N}$, h_k satisfies the conditions (2) and (4) is easily checked. Hence the map h satisfies the conditions (2) and (4). By our step-by-step construction, it also satisfies the conditions (3), (5) and (6). □

Moreover, the degree d and the depth p as constructed above have the followings properties which will be useful in the next sections.

Property 1. *For all* $w, w_1, w_2 \in W$*, if* $w \lhd (w_1, w_2)$ *then* $d(w) = d(w_1)+d(w_2)$.

Proof. Each tuple $(w, w_1, w_2) \in \lhd$ has been added by case 2 or 3 and in both cases the property holds. □

Property 2. *For all* $v, w \in W$ *and* $\alpha \in \Pi$*, if* $vR(\alpha)w$ *then* $d(w) = d(v) + \text{size}(\alpha)$.

Proof. The proof is by induction on the length of α, left to the reader. □

Property 3. *For all* $w, w_1, w_2 \in W$*, if* $w \lhd (w_1, w_2)$ *and* $p(w) \geq 0$ *then* $p(w_1) = p(w_2) = p(w) + 1$.

Proof. Each tuple $(w, w_1, w_2) \in \lhd$ has been added by case 2 or 3. The former case is trivial. In the latter case, as $p(w) \neq -1$, the property holds too. □

Property 4. *For all* $v, w \in W$ *and* $\alpha \in \Pi$*, if* $vR(\alpha)w$ *and* $p(v) \geq 0$ *then* $p(v) = p(w)$.

Proof. By induction on the length of α, left to the reader. □

4 Placeholders and Markers

4.1 Subformulas with Placeholders

Using the same sets Φ_0 and Π_0 of propositional variables and atomic programs as before, the sets Φ^+ and Π^+ of formulas and programs with indices and placeholders are defined by parallel induction:

$$\alpha, \beta := a \mid (\alpha\,;\beta) \mid \varphi? \mid (\alpha \parallel_i \beta)$$
$$\varphi := p \mid (i, j) \mid \bot \mid [\alpha]\varphi$$

where p range over Φ_0, a over Π_0, i over $\mathbb{N}$, j over $\{1, 2\}$, φ over Φ^+ and α and β over Π^+. The integers below the parallel composition symbols are called *indices*. The atomic formulas of the form (i, j) are called *placeholders*. The definitions of lengths and size of Section 2 are extended to Φ^+ and Π^+ by considering placeholders as new propositional variables and ignoring indices.

A formula $\varphi \in \Phi^+$ with indices and placeholders is an *annotated formula with placeholders* if each integer appears at most once as an index in it. The subset $\Phi_{PH} \subset \Phi^+$ of all annotated formula with placeholders is called the *annotated language with placeholders*, and Π_{PH} is the corresponding set of annotated programs with placeholders. For each annotated formula with placeholders $\varphi \in \Phi_{PH}$, $I_\varphi \subseteq \mathbb{N}$ denotes the set of indices appearing in φ.

An annotated formula with placeholders $\varphi \in \Phi_{PH}$ is a *pure annotated formula* if it contains no placeholders. The subset $\Phi_{\mathbb{N}} \subset \Phi_{PH}$ of all pure annotated formula is called the *pure annotated language*, and $\Pi_{\mathbb{N}}$ is the corresponding set of pure annotated programs. There exists a forgetful epimorphism $\overline{\cdot} : \Phi_{\mathbb{N}} \longrightarrow \Phi$ associating to each pure annotated formula $\varphi_{\mathbb{N}}$ the formula $\overline{\varphi_{\mathbb{N}}}$ obtained by removing all indices in $\varphi_{\mathbb{N}}$. $\overline{\varphi_{\mathbb{N}}}$ is called the unannotated formula of $\varphi_{\mathbb{N}}$ and $\varphi_{\mathbb{N}}$ an annotation of $\overline{\varphi_{\mathbb{N}}}$.

Definition 4 (Subformulas with placeholders). *The function* $\mathrm{sf} : \mathbb{N} \times \mathbb{N} \times \Phi_{PH} \longrightarrow \mathcal{P}(\mathbb{N} \times \mathbb{N} \times \Phi_{PH})$ *is inductively defined by:*

$$\begin{aligned}
\mathrm{sf}(d,p,q) &= \{(d,p,q)\} \text{ for all } q \in \Phi_0 \\
\mathrm{sf}(d,p,(i,j)) &= \{(d,p,(i,j))\} \text{ for all } (i,j) \in \mathbb{N} \times \{1,2\} \\
\mathrm{sf}(d,p,\bot) &= \{(d,p,\bot)\} \\
\mathrm{sf}(d,p,[a]\varphi) &= \{(d,p,[a]\varphi)\} \cup \mathrm{sf}(d+1,p,\varphi) \\
\mathrm{sf}(d,p,[\varphi?]\psi) &= \{(d,p,[\varphi?]\psi)\} \cup \mathrm{sf}(d,p,\varphi) \cup \mathrm{sf}(d,p,\psi) \\
\mathrm{sf}(d,p,[\alpha\,;\beta]\varphi) &= \{(d,p,[\alpha\,;\beta]\varphi)\} \cup \mathrm{sf}(d,p,[\alpha][\beta]\varphi) \\
\mathrm{sf}(d,p,[\alpha \parallel_i \beta]\,\varphi) &= \{(d,p,[\alpha \parallel_i \beta]\,\varphi)\} \cup \mathrm{sf}(d,p+1,[\alpha](i,1)) \cup \\
&\quad \mathrm{sf}(d,p+1,[\beta](i,2)) \cup \mathrm{sf}(d+\mathrm{size}(\alpha \parallel \beta),p,\varphi)
\end{aligned}$$

For all pure annotated formula $\varphi \in \Phi_{\mathbb{N}}$ *and* $(d,p,\psi) \in \mathrm{sf}(0,0,\varphi)$, ψ *is called a* subformula with placeholders *of* φ *of degree* d *and depth* p. *The set of all subformulas with placeholders of* φ *is denoted by* $\mathrm{SF}(\varphi)$.

Lemma 7. *For all* $d_1,d_2,p_1,p_2 \in \mathbb{N}$ *and all* $\varphi_1,\varphi_2 \in \Phi_{PH}$:

$$(d_1,p_1,\varphi_1) \in \mathrm{sf}(d_2,p_2,\varphi_2) \Leftrightarrow \mathrm{sf}(d_1,p_1,\varphi_1) \subseteq \mathrm{sf}(d_2,p_2,\varphi_2)$$

Proof. The right to left direction is trivial. The left to right direction is by induction on $|\varphi_2|$. When $\varphi_2 \in \Phi_0 \cup (\mathbb{N} \times \{1,2\})$ or $\varphi_2 = \bot$, $\mathrm{sf}(d_2,p_2,\varphi_2)$ is a singleton hence $(d_1,p_1,\varphi_1) = (d_2,p_2,\varphi_2)$. When $\varphi_2 = [a]\varphi$ then either $(d_1,p_1,\varphi_1) = (d_2,p_2,\varphi_2)$ or $(d_1,p_1,\varphi_1) \in \mathrm{sf}(d_2+1,p_2,\varphi)$ and by induction $\mathrm{sf}(d_1,p_1,\varphi_1) \subseteq \mathrm{sf}(d_2+1,p_2,\varphi) \subseteq \mathrm{sf}(d_2,p_2,\varphi_2)$. The others cases are similar and left to the reader. □

Corollary 1. *For all* $d,p,i \in \mathbb{N}$, $\alpha,\beta \in \Pi_{PH}$ *and* $\varphi,\psi,\varphi_0 \in \Phi_{PH}$,

$$(d,p,[\varphi?]\psi) \in \mathrm{sf}(0,0,\varphi_0) \Rightarrow (d,p,\varphi) \in \mathrm{sf}(0,0,\varphi_0) \tag{13}$$

$$(d,p,[\alpha\,;\beta]\varphi) \in \mathrm{sf}(0,0,\varphi_0) \Rightarrow (d,p,[\alpha][\beta]\varphi) \in \mathrm{sf}(0,0,\varphi_0) \tag{14}$$

$$(d,p,[\alpha \parallel_i \beta]\,\varphi) \in \mathrm{sf}(0,0,\varphi_0) \Rightarrow (d,p+1,[\alpha](i,1)) \in \mathrm{sf}(0,0,\varphi_0) \tag{15}$$

$$(d,p,[\alpha \parallel_i \beta]\,\varphi) \in \mathrm{sf}(0,0,\varphi_0) \Rightarrow (d,p+1,[\beta](i,2)) \in \mathrm{sf}(0,0,\varphi_0) \tag{16}$$

Proof. The proof is given for (14) only. The other implications are similar and left to the reader. By Lemma 7, $(d,p,[\alpha\,;\beta]\varphi) \in \mathrm{sf}(0,0,\varphi_0) \Rightarrow \mathrm{sf}(d,p,[\alpha\,;\beta]\varphi) \subseteq \mathrm{sf}(0,0,\varphi_0)$. By construction, $\mathrm{sf}(d,p,[\alpha][\beta]\varphi) \subseteq \mathrm{sf}(d,p,[\alpha\,;\beta]\varphi)$. And by Lemma 7 again, $(d,p,[\alpha][\beta]\varphi) \in \mathrm{sf}(d,p,[\alpha\,;\beta]\varphi)$. □

Lemma 8. *For all* $d,p \in \mathbb{N}$, $\alpha \in \Pi_{PH}$ *and* $\varphi,\psi \in \Phi_{PH}$, *if* $(d,p,[\alpha]\varphi) \in \mathrm{sf}(0,0,\psi)$ *then* $(d+\mathrm{size}(\alpha),p,\varphi) \in \mathrm{sf}(0,0,\psi)$.

Proof. The proof is by induction on the length of α. Each case is similar to the proof of Corollary 1, using Lemma 7 twice. They are all left to the reader. □

Lemma 9. *For all pure annotated formula* $\varphi \in \Phi_{\mathbb{N}}$, *the cardinality of* $\mathrm{sf}(0,0,\varphi)$ *is linear in the number of occurences of symbols in the unannotated formula* $\overline{\varphi}$.

Proof. A value is assigned to each symbol in any annotated formula with placeholders: 3 for $\|$; 1 for propositional variables, commas, $\bot$, atomic programs, semicolons and question marks; 0 for anything else (braces, parentheses and integers). For all annotated formula with placeholders $\varphi \in \Phi_{PH}$, let $L(\varphi)$ be the sum of those values for each occurence of symbols in φ. Obviously, for all pure annotated formula $\varphi \in \Phi_{\mathbb{N}}$, $L(\varphi)$ is less or equal to three times the number of occurences of symbols in the unannotated formula $\overline{\varphi}$. Moreover, it can be easily proved by induction on $L(\varphi)$, that for all $d, p \in \mathbb{N}$ and all annotated formula with placeholders $\varphi \in \Phi_{PH}$, the cardinality of $\mathrm{sf}(d, p, \varphi)$ is equal to $L(\varphi)$. □

Lemma 10. *For all $d, p \in \mathbb{N}$, $\varphi \in \Phi_{\mathbb{N}}$ and $(d', p', \varphi') \in \mathrm{sf}(d, p, \varphi)$:*

$$d' \leq d + |\varphi| \tag{17}$$
$$p' \leq p + |\varphi| \tag{18}$$

Proof. The proof is by induction on $|\varphi|$. The base cases, for propositional variables, placeholders and $\bot$, are trivial. If $(d', p', \varphi') \in \mathrm{sf}(d, p, [a]\varphi)$, then either $(d', p', \varphi') = (d, p, [a]\varphi)$ or $(d', p', \varphi') \in \mathrm{sf}(d+1, p, \varphi)$ and by induction $d' \leq d+1+|\varphi| = d+|[a]\varphi|$ and $p' \leq p+|\varphi| \leq p+|[a]\varphi|$. For tests and sequential compositions, the proof is direct by induction and left to the reader.

If $(d', p', \varphi') \in \mathrm{sf}\,(d, p, [\alpha \parallel_i \beta]\,\varphi)$, then either $(d', p', \varphi') = (d, p, [\alpha \parallel_i \beta]\,\varphi)$ or one of the following holds:

$$(d', p', \varphi') \in \mathrm{sf}(d, p+1, [\alpha](i, 1)) \tag{19}$$
$$(d', p', \varphi') \in \mathrm{sf}(d, p+1, [\beta](i, 2)) \tag{20}$$
$$(d', p', \varphi') \in \mathrm{sf}(d + \mathrm{size}\,(\alpha \parallel_i \beta), p, \varphi) \tag{21}$$

If (19) holds, as $|[\alpha](i,1)| < |[\alpha \parallel_i \beta]\,\varphi| = |\alpha| + 1 + |\beta| + |\varphi|$, properties (17) and (18) are verified by induction. The proof is identical if (20) holds. If (21) holds, by induction, $d' \leq d + \mathrm{size}\,(\alpha \parallel_i \beta) + |\varphi|$ and $p' \leq p + |\varphi| < p + |[\alpha \parallel_i \beta]\,\varphi|$. And by Lemma 2, $\mathrm{size}\,(\alpha \parallel_i \beta) + |\varphi| \leq |[\alpha \parallel_i \beta]\,\varphi|$. □

Definition 5 (Annotated subprograms). *Given a pure annotated formula $\varphi_0 \in \Phi_{\mathbb{N}}$, the set* $\mathrm{SP}\,(\varphi_0)$ *of* φ_0's annotated subprograms *is defined as*

$$\mathrm{SP}\,(\varphi_0) = \{\alpha \in \Pi_{PH} \mid \exists \varphi \in \Phi_{PH},\ [\alpha]\varphi \in \mathrm{SF}(\varphi_0)\}$$

Lemma 11. *No placeholders appear in any annotated subprogram.*

Proof. Let Φ_S be the smallest language containing $\bot$, all propositional variables and placeholders from Φ_{PH} and such that for all $\alpha \in \Pi_{\mathbb{N}}$ and $\varphi \in \Phi_S$, $[\alpha]\varphi \in \Phi_S$. Obviously, $\Phi_{\mathbb{N}} \subset \Phi_S \subset \Phi_{PH}$. By induction on $|\varphi|$, the following property can be easily proved:

$$\forall \varphi \in \Phi_S, \forall d, p \in \mathbb{N}, \forall (d', p', \psi) \in \mathrm{sf}(d, p, \varphi),\ \psi \in \Phi_S$$

Therefore, for all $[\alpha]\varphi \in \mathrm{SF}(\varphi_0)$, $\alpha \in \Pi_{\mathbb{N}}$. □

4.2 Model extension with Markers

Let $\mathcal{M} = (W, R, \lhd, V)$ be a model on Φ. The sets $\Phi^+_{\mathcal{M}}$ and $\Pi^+_{\mathcal{M}}$ of formulas and programs with indices and markers from $\mathcal{M}$ are defined by parallel induction:

$$\begin{aligned} \alpha, \beta &:= a \mid (\alpha\,;\beta) \mid \varphi? \mid (\alpha \parallel_i \beta) \\ \varphi &:= p \mid w \mid \bot \mid [\alpha]\varphi \end{aligned}$$

where p range over Φ_0, a over Π_0, i over $\mathbb{N}$, w over W, φ over $\Phi^+_{\mathcal{M}}$ and α and β over $\Pi^+_{\mathcal{M}}$. The atomic formulas belonging to W are called *markers*. The definitions of lengths and size of Section 2 are extended to $\Phi^+_{\mathcal{M}}$ and $\Pi^+_{\mathcal{M}}$ by considering markers as new propositional variables and ignoring indices.

A formula $\varphi \in \Phi^+_{\mathcal{M}}$ is an *annotated formula with markers from* $\mathcal{M}$ if each integer appears at most once as index in it. The subset $\Phi_{\mathcal{M}} \subset \Phi^+_{\mathcal{M}}$ of all annotated formula with markers from $\mathcal{M}$ is called the *annotated language with markers from* $\mathcal{M}$, and $\Pi_{\mathcal{M}}$ is the corresponding set of annotated programs with markers from $\mathcal{M}$. A formula $\varphi \in \Phi_{\mathcal{M}}$ is *pure* iff it contains no markers. It is worth noting that the subset of pure formulas from $\Phi_{\mathcal{M}}$ is the language of pure annotated formula $\Phi_{\mathbb{N}}$.

The *extension of* $\mathcal{M}$ *with markers* is the model $\mathcal{M}^+ = (W, R, \lhd, V^+)$ on the language $\Phi_{\mathcal{M}}$ with the new valuation V^+ defined as follows:

$$\begin{aligned} V^+(p) &= V(p) \qquad \text{if } p \in \Phi_0 \\ V^+(w) &= W \setminus \{w\} \text{ if } w \in W \end{aligned}$$

Lemma 12. *For all $\varphi \in \Phi_{\mathcal{M}}$, if φ is pure then for all $w \in W$, $\mathcal{M}, w \vDash \overline{\varphi} \Leftrightarrow \mathcal{M}^+, w \vDash \varphi$.*

Proof. By induction on φ, left to the reader.

Definition 6. *Given a pure annotated formula $\varphi \in \Phi_{\mathbb{N}}$ and a model $\mathcal{M} = (W, R, \lhd, V)$,* a binding *for φ on $\mathcal{M}$ is a partial function $m : I_\varphi \times \{1, 2\} \longrightarrow W$. The set of all such bindings is denoted by $B^{\mathcal{M}}_{\varphi}$.*

Given a pure annotated formula $\varphi_0 \in \Phi_{\mathbb{N}}$, a model $\mathcal{M} = (W, R, \lhd, V)$ and a binding $m \in B^{\mathcal{M}}_{\varphi_0}$, the partial function $F_{\varphi_0,\mathcal{M},m} : \mathrm{SF}(\varphi_0) \longrightarrow \Phi_{\mathcal{M}}$ is defined inductively by:

$$\begin{aligned} F_{\varphi_0,\mathcal{M},m}(p) &= p && \text{if } p \in \Phi_0 \\ F_{\varphi_0,\mathcal{M},m}(\bot) &= \bot \\ F_{\varphi_0,\mathcal{M},m}((i,k)) &= m(i,k) && \text{if } m(i,k) \text{ is defined} \\ F_{\varphi_0,\mathcal{M},m}([\alpha]\varphi) &= [\alpha]\, F_{\varphi_0,\mathcal{M},m}(\varphi) && \text{if } F_{\varphi_0,\mathcal{M},m}(\varphi) \text{ is defined} \\ F_{\varphi_0,\mathcal{M},m}(\varphi) &\text{ is undefined} && \text{otherwise} \end{aligned}$$

When it does not lead to confusion we will write F_m instead of $F_{\varphi_0,\mathcal{M},m}$.

Procedure 1: Selection of a finite submodel

Input: An annotated formula $\varphi_a \in \Phi_{\mathcal{M}_u}$ satisfiable in $\mathcal{M}$ at $w_u \in W$; a function $E : W \times B_{\varphi_a}^{\mathcal{M}_u} \longrightarrow \mathcal{P}(\Phi_{\mathcal{M}_u})$.

Result: $\mathcal{S}$ a tree with nodes belonging to $W \times B_{\varphi_a}^{\mathcal{M}_u}$.

1 **initialisation**
2 $\quad\mathcal{S}$ = the one (unmarked) node tree $\{(w_u, \emptyset)\}$
3 **while** *some nodes in* $\mathcal{S}$ *are not marked* **do**
4 $\quad$**choose** an unmarked node (w, m) from $\mathcal{S}$
5 $\quad$**mark** (w, m)
6 $\quad$**foreach** $[a]\varphi \in E(w, m)$ *s.t.* $\mathcal{M}, w \not\models [a]\varphi$ **do**
7 $\quad\quad$**choose** w' **s.t.** $wR(a)w'$ and $\mathcal{M}, w' \not\models \varphi$
8 $\quad\quad$**add** (w', m) **as** (w, m)'s child in $\mathcal{S}$
9 $\quad$**foreach** $[\alpha \parallel_i \beta]\varphi \in E(w, m)$ *s.t.* $\mathcal{M}, w \not\models [\alpha \parallel_i \beta]\varphi$ **do**
10 $\quad\quad$**choose** w_1, w_2, w_3, w_4, w_5 **s.t.**
11 $\quad\quad\quad w \lhd (w_1, w_2) \wedge w_1 R(\alpha) w_3 \wedge w_2 R(\beta) w_4 \wedge w_5 \lhd (w_3, w_4) \wedge \mathcal{M}, w_5 \not\models \varphi$
12 $\quad\quad$**add** $(w_1, m \uplus \{((i, 1), w_3)\})$ **as** (w, m)'s child in $\mathcal{S}$
13 $\quad\quad$**add** $(w_2, m \uplus \{((i, 2), w_4)\})$ **as** (w, m)'s child in $\mathcal{S}$
14 $\quad\quad$**if** $w_5 \neq w$ **then**
15 $\quad\quad\quad$**add** (w_5, m) **as** (w, m)'s child in $\mathcal{S}$

5 Finite Model Property by Selection

Let us consider a formula $\varphi_0 \in \Phi$. If φ_0 is satisfiable, thanks to the Löwenheim-Skolem theorem, there exists a countable model $\mathcal{M}_0 = (W_0, R_0, \lhd_0, V_0)$ and a world $w_0 \in W_0$ such that $\mathcal{M}_0, w_0 \vDash \varphi_0$. Let $\mathcal{M}_u = (W_u, R_u, \lhd_u, V_u)$ be the unfolding of $\mathcal{M}_0$ at w_0 with root w_u, degree $d : W_u \longrightarrow \mathbb{Q}$ and depth $p : W_u \longrightarrow \mathbb{Z}$ as defined in Section 3. Let $\mathcal{M} = (W, R, \lhd, V)$ be the extension with markers of $\mathcal{M}_u$. As $W = W_u$, degree and depth apply to worlds of $\mathcal{M}$ too. Let $\varphi_a \in \Phi_{\mathbb{N}}$ be an annotation of φ_0. As φ_a is pure, by Lemma 12, $\mathcal{M}, w_u \vDash \varphi_a$.

Procedure 1 constructs a tree $\mathcal{S}$ whose nodes are tuples from $W \times B_{\varphi_a}^{\mathcal{M}_u}$. The function $E : W \times B_{\varphi_a}^{\mathcal{M}_u} \longrightarrow \mathcal{P}(\Phi_{\mathcal{M}_u})$ associates to each node from $\mathcal{S}$ the set of φ_a's annotated subformulas with markers which have to be considered to add children to this node. It is defined as:

$$E(w, m) = \{F_m(\varphi) \mid \exists d', p',\ (d', p', \varphi) \in \mathrm{sf}(0, 0, \varphi_a) \wedge d(w) \leq d' \wedge p(w) = p'\}$$

Lemma 13. *For all* $(w, m) \in \mathcal{S}$, $p(w) \geq 0$.

Proof. The proof is by induction on $\mathcal{S}$: the root's depth is 0 and for each child (w', m') of (w, m), if $p(w) \geq 0$ then $p(w') \geq 0$. If (w', m') has been added at line 8, then $wR(a)w'$ and by Property 4, $p(w') = p(w)$. The proof is identical if (w', m') has been added at line 15. If (w', m') has been added at line 12, there exists $w_2 \in W$ such that $w \lhd (w', w_2)$ and by Property 3, $p(w') = p(w) + 1$. The proof is identical if (w', m') has been added at line 13. □

Lemma 14. *The size of* $\mathcal{S}$ *is bounded by an exponential in the number of occurences of symbols in* φ_0.

Proof. The vertex degree of $\mathcal{S}$ is bounded by the cardinality of $\mathrm{sf}(0,0,\varphi_a)$ multiplied by three. Lemma 9 proved the cardinality of $\mathrm{sf}(0,0,\varphi_a)$ is linear in the number of occurences of symbols in φ_0. The remaining of the proof is devoted to demonstrate the length of the path from the root $(w_u,\emptyset)$ to any leaf is bounded by a quadratic function on the number of occurences of symbols in φ_0.

We first define the following maximal elements:

$$d_{\max} = \max\{d \in \mathbb{N} \mid \exists p,\varphi,\ (d,p,\varphi) \in \mathrm{sf}(0,0,\varphi_a)\}$$
$$p_{\max} = \max\{p \in \mathbb{N} \mid \exists d,\varphi,\ (d,p,\varphi) \in \mathrm{sf}(0,0,\varphi_a)\}$$

Clearly, if $d(w) > d_{\max}$ or $p(w) > p_{\max}$ for a given node $(w,m) \in \mathcal{S}$, then $E(w,m) = \emptyset$ and (w,m,t) has no children in $\mathcal{S}$. Moreover, by Lemmas 10 and 1, both $d_{\max}$ and $p_{\max}$ are less or equal than the number of occurences of symbols in φ_0.

We define the function $f : \mathcal{S} \longrightarrow \mathbb{Q}$ by:

$$f(w,m) = (d_{\max}+1).p(w) + d(w)$$

Obviously, if $f(w,m) \geq (d_{\max}+1)(p_{\max}+1)$ for a given node $(w,m) \in \mathcal{S}$, then this node has no children in $\mathcal{S}$. We will prove that for any child (w',m') of (w,m) in $\mathcal{S}$, $f(w',m') \geq f(w,m)+1$.

If (w',m') has been added as (w,m)'s child at line 8, then $wR(a)w'$ and by Lemma 13 and Properties 2 and 4, $d(w') = d(w)+1$ and $p(w') = p(w)$. Hence $f(w',m') = f(w,m)+1$.

If (w',m') has been added as (w,m)'s child at line 12, then $\exists w_2 \in W$ such that $w \lhd (w',w_2)$. By Lemma 13 and Property 3, $p(w') = p(w)+1$, thus $f(w',m') \geq (d_{\max}+1).p(w) + d_{\max} + 1$. And since (w,m) has children, $d(w) \leq d_{\max}$. The proof is identical if (w',m') has been added at line 13.

If (w',m') has been added as (w,m)'s child at line 15, then $wR(\alpha \parallel_i \beta)w'$ and by Lemma 13 and Properties 2 and 4, $d(w') = d(w) + \mathrm{size}(\alpha \parallel_i \beta)$ and $p(w') = p(w)$, hence $f(w',m') = f(w,m) + \mathrm{size}(\alpha \parallel_i \beta)$. Moreover, $\mathrm{size}(\alpha \parallel_i \beta) \geq 1$ because otherwise, by Lemmas 3 and 5, $w' = w$ which is impossible by the condition at line 14. □

From the tree $\mathcal{S}$ produced by Procedure 1, the model $\mathcal{M}_f = (W_f, R_f, \lhd_f, V_f)$ is defined with W_f being the subset $\{w \in W \mid \exists m,\ (w,m) \in \mathcal{S}\}$ and R_f, $\lhd_f$ and V the restriction of R, $\lhd$ and V to W_f. Obviously, $\mathcal{M}_f$ is finite and $w_u \in W_f$. Let $E^+(w) = \bigcup_{m \mid (w,m)\in\mathcal{S}} E(w,m)$ for all $w \in W_f$.

Lemma 15. *The model $\mathcal{M}_f$ is $\lhd$-separated and $\lhd$-deterministic.*

Proof. By Lemma 5, $\mathcal{M}_u$ is $\lhd$-separated and $\lhd$-deterministic. Since both this conditions are universal and $\mathcal{M}_f$ is a submodel of $\mathcal{M}_u$, $\mathcal{M}_f$ is $\lhd$-separated and $\lhd$-deterministic. □

Lemma 16 (Truth lemma). $\forall w \in W_f$*:*

$$\forall \varphi \in E^+(w), \varphi \text{ pure},\ \mathcal{M}, w \vDash \varphi \Rightarrow \mathcal{M}_f, w \vDash \varphi \quad (22)$$
$$\forall \varphi \in E^+(w),\ \mathcal{M}, w \vDash \varphi \Leftarrow \mathcal{M}_f, w \vDash \varphi \quad (23)$$
$$\forall v \in W_f, \forall (d', p(v), [\alpha]\varphi) \in \mathrm{sf}(0,0,\varphi_a), d(v) \leq d',\ vR(\alpha)w \Leftarrow vR_f(\alpha)w \quad (24)$$

Proof. The proof is by parallel induction on the length of φ for (22) and (23) and on the length of α for (24).

Hypothesis (22). The base cases for $\bot$ and propositional variables are trivial.

Suppose $\mathcal{M}, w \vDash [a]\varphi$, $[a]\varphi \in E^+(w)$, $[a]\varphi$ is pure and $wR_f(a)v$. Then there exists d' and p' such that $(d', p', [a]\varphi) \in \mathrm{sf}(0,0,\varphi_a)$, $d(w) \leq d'$ and $p(w) = p'$. By hypothesis (24), $wR(a)v$ and hence $\mathcal{M}, v \vDash \varphi$. By Property 2, $d(v) = d(w) + 1$ and by Lemma 13 and Property 4, $p(v) = p(w)$. By Lemma 8, $(d'+1, p', \varphi) \in \mathrm{sf}(0,0,\varphi_a)$. As $d(v) \leq d'+1$, $p(v) = p'$ and φ is pure, $\varphi \in E^+(v)$. By induction, $\mathcal{M}_f, v \vDash \varphi$.

Suppose $\mathcal{M}, w \vDash [\alpha\,;\beta]\varphi$, $[\alpha\,;\beta]\varphi \in E^+(w)$ and $[\alpha\,;\beta]\varphi$ is pure. Then there exists $d' \geq d(w)$ such that $(d', p(w), [\alpha\,;\beta]\varphi) \in \mathrm{sf}(0,0,\varphi_a)$. By Corollary 1, $(d', p(w), [\alpha][\beta]\varphi) \in \mathrm{sf}(0,0,\varphi_a)$ and thus $[\alpha][\beta]\varphi \in E^+(\varphi_a)$. Since $|[\alpha][\beta]\varphi| < |[\alpha\,;\beta]\varphi|$ and $\mathcal{M}, w \vDash [\alpha][\beta]\varphi$, by induction, $\mathcal{M}_f, w \vDash [\alpha][\beta]\varphi$.

Suppose $\mathcal{M}, w \vDash [\varphi?]\psi$, $[\varphi?]\psi \in E^+(w)$ and $[\varphi?]\psi$ is pure. Then there exists $d' \geq d(w)$ such that $(d', p(w), [\varphi?]\psi) \in \mathrm{sf}(0,0,\varphi_a)$. By Corollary 1 and Lemma 8 $(d', p(w), \varphi)$ and $(d', p(w), \psi)$ belong to $\mathrm{sf}(0,0,\varphi_a)$. Thus φ and ψ belong to $E^+(w)$. If $\mathcal{M}, w \nvDash \varphi$ then by induction hypothesis (23), $\mathcal{M}_f, w \nvDash \varphi$. If $\mathcal{M}, w \vDash \psi$, by induction hypothesis (22), $\mathcal{M}_f, w \vDash \psi$.

Suppose $\mathcal{M}, w \vDash [\alpha \parallel_i \beta]\,\varphi$, $[\alpha \parallel_i \beta]\,\varphi \in E^+(w)$, $wR_f\,(\alpha \parallel_i \beta)\,v$ and $[\alpha \parallel_i \beta]\,\varphi$ is pure. Then there exists $d' \geq d(w)$ such that $(d', p(w), [\alpha \parallel_i \beta]\,\varphi) \in \mathrm{sf}(0,0,\varphi_a)$. By hypothesis (24), $wR\,(\alpha \parallel_i \beta)\,v$ and hence $\mathcal{M}, w \vDash \varphi$. By Property 2, $d(v) = d(w) + \mathrm{size}\,(\alpha \parallel_i \beta)$ and by Lemma 13 and Property 4, $p(v) = p(w)$. By Lemma 8, $(d' + \mathrm{size}\,(\alpha \parallel_i \beta)\,, p(w), \varphi) \in \mathrm{sf}(0,0,\varphi_a)$. As $d(v) \leq d' + \mathrm{size}\,(\alpha \parallel_i \beta)$, $p(v) = p(w)$ and φ is pure, $\varphi \in E^+(v)$. By induction, $\mathcal{M}_f, v \vDash \varphi$.

Hypothesis (23). The base cases for $\bot$, propositional variables and markers are trivial.

Suppose $\mathcal{M}, w \nvDash [a]\varphi$ and $[a]\varphi \in E^+(w)$. Then there exists $(w, m) \in \mathcal{S}$ such that $[a]\varphi \in E(w, m)$. By construction of $\mathcal{S}$ there exists $w' \in W$ such that $wR(a)w'$, $\mathcal{M}, w' \nvDash \varphi$ and $(w', m) \in \mathcal{S}$, thus $wR_f(a)w'$. Moreover, there exists $\psi \in \mathrm{SF}(\varphi_a)$ and $d' \geq d(w)$ such that $F_m(\psi) = \varphi$ and $(d', p(w), [a]\psi) \in \mathrm{sf}(0,0,\varphi_a)$. By Lemma 8, $(d'+1, p(w), \psi) \in \mathrm{sf}(0,0,\varphi_a)$ and by Lemma 13 and Properties 2 and 4, $d(w') = d(w) + 1$ and $p(w') = p(w)$. Hence $\varphi \in E^+(w')$ and by induction $\mathcal{M}_f, w' \nvDash \varphi$. Consequently $\mathcal{M}_f, w \nvDash [\alpha]\varphi$.

Suppose $\mathcal{M}, w \nvDash [\alpha\,;\beta]\varphi$ and $[\alpha\,;\beta]\varphi \in E^+(w)$. Then there exists $(w, m) \in \mathcal{S}$, $\psi \in \mathrm{SF}(\varphi_a)$ and $d' \geq d(w)$ such that $F_m(\psi) = \varphi$ and $(d', p(w), [\alpha\,;\beta]\psi) \in \mathrm{sf}(0,0,\varphi_a)$. By Corollary 1, $(d', p(w), [\alpha][\beta]\psi) \in \mathrm{sf}(0,0,\varphi_a)$. Thus $[\alpha][\beta]\psi \in E^+(w)$ and by induction $\mathcal{M}_f, w \nvDash [\alpha][\beta]\varphi$.

Suppose $\mathcal{M}, w \nvDash [\varphi?]\psi$ and $[\varphi?]\psi \in E^+(w)$. Then both $\mathcal{M}, w \vDash \varphi$ and $\mathcal{M}, w \nvDash \psi$ hold. Therefore there exists $(w, m) \in \mathcal{S}$, $\psi' \in \mathrm{SF}(\varphi_a)$ and $d' \geq d(w)$ such that $F_m(\psi') = \psi$ and $(d', p(w), [\varphi?]\psi') \in \mathrm{sf}(0,0,\varphi_a)$. By Corollary 1 and Lemma 8, $(d', p(w), \varphi)$ and $(d', p(w), \psi')$ both belong to $\mathrm{sf}(0,0,\varphi_a)$. And by induction hypothesis (22) and (23), $\mathcal{M}_f, w \vDash \varphi$ and $\mathcal{M}_f, w \nvDash \psi$.

Suppose $\mathcal{M}, w \nvDash [\alpha \parallel_i \beta]\,\varphi$ and $[\alpha \parallel_i \beta]\,\varphi \in E^+(w)$. Then there exists $\psi \in \mathrm{SF}(\varphi_a)$, $(w, m) \in \mathcal{S}$ and $d' \geq d(w)$ such that $(d', p(w), [\alpha \parallel_i \beta]\,\psi) \in \mathrm{sf}(0,0,\varphi_a)$

and $F_m(\psi) = \varphi$. By construction, there exists $w_1, w_2, w_3, w_4, w_5 \in W$ such that $w \lhd (w_1, w_2)$, $w_1 R(\alpha) w_3$, $w_2 R(\beta) w_4$, $w_5 \lhd (w_3, w_4)$, $\mathcal{M}, w_5 \not\models \varphi$, $(w_1, m_1) \in \mathcal{S}$, $(w_2, m_2) \in \mathcal{S}$ and $(w_5, m) \in \mathcal{S}$, with $m_1 = m \uplus \{((i,1), w_3)\}$ and $m_2 = m \uplus \{((i,2), w_4)\}$. By Lemma 8, $(d' + \text{size}(\alpha \parallel_i \beta), p(w), \varphi) \in \text{sf}(0,0,\varphi_a)$ and by Lemma 13 and Properties 2 and 4, $d(w_5) = d(w) + \text{size}(\alpha \parallel_i \beta)$ and $p(w_5) = p(w)$, then by induction hypothesis (23), $\mathcal{M}_f, w_5 \not\models \varphi$. It remains to prove that $w R_f (\alpha \parallel_i \beta) w_5$. By Corollary 1, both $(d', p(w)+1, [\alpha](i,1))$ and $(d', p(w)+1, [\alpha](i,2))$ belong to $\text{sf}(0,0,\varphi_a)$. By Lemma 13 and Properties 1 and 3, $d(w_1) \leq d(w)$, $d(w_2) \leq d(w)$ and $p(w_1) = p(w_2) = p(w)+1$. Therefore $[\alpha] w_3 \in E(w_1, m_1)$ and $[\beta] w_4 \in E(w_2, m_2)$. Thus by induction hypothesis (23), w_3 and w_4 belongs to W_f, $w_1 R_f(\alpha) w_3$ and $w_2 R_f(\beta) w_4$. Therefore, $w R_f(\alpha \parallel_i \beta) w_5$.

Hypothesis (24). The base case for atomic programs is trivial.

Suppose $v R_f(\alpha \,;\, \beta) w$, $(d', p(v), [\alpha \,;\, \beta]\varphi) \in \text{sf}(0,0,\varphi_a)$ and $d' \geq d(v)$. Then there exists $w' \in W_f$ such that $v R_f(\alpha) w'$ and $w' R_f(\alpha) w$. By Corollary 1, $(d', p(v), [\alpha][\beta]\varphi) \in \text{sf}(0,0,\varphi_a)$. By induction hypothesis (24), $v R(\alpha) w'$. Thanks to Lemma 13 and Properties 2 and 4, $d(w') = d(v) + \text{size}(\alpha)$ and $p(w') = p(v)$. By Lemma 8, $(d' + \text{size}(\alpha), p(v), [\beta]\varphi) \in \text{sf}(0,0,\varphi_a)$ and by induction hypothesis (24), $w' R(\beta) w$. Since $v R(\alpha) w'$, $v R(\alpha \,;\, \beta) w$.

Suppose $v R_f(\psi?) w$, $(d', p(v), [\psi?]\varphi) \in \text{sf}(0,0,\varphi_a)$ and $d' \geq d(v)$. Then $w = v$ and as ψ is pure by Lemma 11, $\mathcal{M}_f, v \vDash \psi$. By Corollary 1, $(d', p(v), \psi) \in \text{sf}(0,0,\varphi_a)$. As $|\psi?| > |\psi|$, by induction hypothesis (23), $\mathcal{M}, v \vDash \psi$. Since $v = w$, $v R(\psi?) w$.

Suppose $v R_f(\alpha \parallel_i \beta) w$, $(d', p(v), [\alpha \parallel_i \beta]\varphi) \in \text{sf}(0,0,\varphi_a)$ and $d' \geq d(v)$. Then there exists $w_1, w_2, w_3, w_4 \in W_f$ such that $v \lhd_f (w_1, w_2)$, $w_1 R_f(\alpha) w_3$, $w_2 R_f(\beta) w_4$ and $w \lhd_f (w_3, w_4)$. Obviously, both $v \lhd (w_1, w_2)$ and $w \lhd (w_3, w_4)$ hold. By Corollary 1, both $(d', p(v)+1, [\alpha](i,1))$ and $(d', p(v)+1, [\beta](i,2))$ belong to $\text{sf}(0,0,\varphi_a)$. By Lemma 13 and Properties 1 and 3, $d(w_1) \leq d(v)$, $d(w_2) \leq d(v)$ and $p(w_1) = p(w_2) = p(v) + 1$. Thus, by induction hypothesis (24), $w_1 R(\alpha) w_3$ and $w_2 R(\beta) w_4$. Then $v R(\alpha \parallel_i \beta) w$. □

Proposition 2. *The satisfiability problem of PPDL$_0^{det}$'s formulas interpreted in $\lhd$-separated $\lhd$-deterministic models is in NEXPTIME.*

Proof. Lemmas 14, 15 and 16 prove that whenever a formula φ is satisfiable in a $\lhd$-separated $\lhd$-deterministic model, φ is satisfiable in a $\lhd$-deterministic $\lhd$-separated model with size exponential in the number of occurences of symbols.

6 Conclusion

We have proved the fragment $\text{PPDL}_0^{\text{det}}$ of PRSPDL is decidable, giving a NEXPTIME complexity upper bound. Because of the subtleties brought about by the parallel composition, we have used placeholders and markers in the selection procedure. We expect this technique could be reused to express subformulas in other fragments of PRSPDL.

Still, the exact complexity of $\mathrm{PPDL}_0^{\mathrm{det}}$ is unknown. The only known lower bound is given by the straightforward embeding of the modal logic **K**, resulting in $\mathrm{PPDL}_0^{\mathrm{det}}$ being PSPACE-hard [11].

Althought the $\lhd$-separation condition is needed for the axiomatization of PRSPDL_0 [1], we believe this condition makes the satisfiability problem harder. We conjecture the satisfiability problem of the same language interpreted on $\lhd$-deterministic models to be PSPACE-complete, leaving the proof as future work.

References

1. Balbiani, P., Boudou, J.: Iteration-free PDL with storing, recovering and parallel composition: a complete axiomatization, submitted
2. Balbiani, P., Tinchev, T.: Definability and computability for PRSPDL. In: Advances in Modal Logic (2014), to appear
3. Benevides, M.R.F., de Freitas, R.P., Viana, J.P.: Propositional dynamic logic with storing, recovering and parallel composition. Electr. Notes Theor. Comput. Sci. 269, 95–107 (2011)
4. Blackburn, P., de Rijke, M., Venema, Y.: Modal Logic, Cambridge Tracts in Theoretical Computer Science, vol. 53. Cambridge University Press (2001)
5. Brookes, S.: A semantics for concurrent separation logic. Theor. Comput. Sci. 375(1-3), 227–270 (2007)
6. Brotherston, J., Kanovich, M.I.: Undecidability of propositional separation logic and its neighbours. In: LICS. pp. 130–139. IEEE Computer Society (2010)
7. Fischer, M.J., Ladner, R.E.: Propositional dynamic logic of regular programs. J. Comput. Syst. Sci. 18(2), 194–211 (1979)
8. Galmiche, D., Larchey-Wendling, D.: Expressivity properties of boolean BI through relational models. In: FSTTCS. Lecture Notes in Computer Science, vol. 4337, pp. 357–368. Springer Berlin Heidelberg (2006)
9. Goldblatt, R.: Logics of Time and Computation. Center for the Study of Language and Information (1987)
10. Harel, D., Kozen, D., Tiuryn, J.: Dynamic logic. MIT press (2000)
11. Ladner, R.E.: The computational complexity of provability in systems of modal propositional logic. SIAM J. Comput. 6(3), 467–480 (1977)
12. Larchey-Wendling, D., Galmiche, D.: Exploring the relation between Intuitionistic BI and Boolean BI: an unexpected embedding. Mathematical Structures in Computer Science 19(3), 435–500 (2009)
13. Larchey-Wendling, D., Galmiche, D.: The undecidability of boolean BI through phase semantics. In: LICS. pp. 140–149. IEEE Computer Society (2010)
14. O'Hearn, P.W.: Resources, concurrency, and local reasoning. Theor. Comput. Sci. 375(1-3), 271–307 (2007)
15. Pym, D.J.: The semantics and proof theory of the logic of bunched implications, vol. 26. Springer (2002)
16. Reynolds, J.C.: Separation logic: A logic for shared mutable data structures. In: LICS. pp. 55–74. IEEE Computer Society (2002)