Decidable Entailments in Separation Logic with Inductive Definitions: Beyond Establishment

Mnacho Echenim
Univ. Grenoble Alpes, CNRS, LIG, F-38000 Grenoble France

Radu Iosif
Univ. Grenoble Alpes, CNRS, VERIMAG, F-38000 Grenoble France

Nicolas Peltier
Univ. Grenoble Alpes, CNRS, LIG, F-38000 Grenoble France

Abstract

We define a class of Separation Logic [10, 16] formulæ, whose entailment problem *given formulæ* $\phi, \psi_1, \ldots, \psi_n$, *is every model of* ϕ *a model of some* ψ_i*?* is 2-EXPTIME-complete. The formulæ in this class are existentially quantified separating conjunctions involving predicate atoms, interpreted by the least sets of store-heap structures that satisfy a set of inductive rules, which is also part of the input to the entailment problem. Previous work [8, 12, 15] consider *established* sets of rules, meaning that every existentially quantified variable in a rule must eventually be bound to an *allocated* location, i.e. from the domain of the heap. In particular, this guarantees that each structure has treewidth bounded by the size of the largest rule in the set. In contrast, here we show that establishment, although sufficient for decidability (alongside two other natural conditions), is not necessary, by providing a condition, called *equational restrictedness*, which applies syntactically to (dis-)equalities. The entailment problem is more general in this case, because equationally restricted rules define richer classes of structures, of unbounded treewidth. In this paper we show that (1) every established set of rules can be converted into an equationally restricted one and (2) the entailment problem is 2-EXPTIME-complete in the latter case, thus matching the complexity of entailments for established sets of rules [12, 15].

2012 ACM Subject Classification Theory of computation → Logic and verification

Keywords and phrases Separation logic, Induction definitions, Inductive theorem proving, Entailments, Complexity

Digital Object Identifier 10.4230/LIPIcs...

1 Introduction

Separation Logic (SL) [10, 16] is widely used to reason about programs manipulating recursively linked data structures, being at the core of several industrial-scale static program analysis techniques [3, 2, 5]. Given an integer $\mathfrak{K} \geq 1$, denoting the number of fields in a record datatype, and an infinite set $\mathbb{L}$ of memory locations (addresses), the assertions in this logic describe *heaps*, that are finite partial functions mapping locations to records, i.e., $\mathfrak{K}$-tuples of locations. A location ℓ in the domain of the heap is said to be *allocated* and the *points-to* atom $x \mapsto (y_1, \ldots, y_{\mathfrak{K}})$ states that the location associated with x refers to the tuple of locations associated with $(y_1, \ldots, y_{\mathfrak{K}})$. The *separating conjunction* $\phi * \psi$ states that the formulæ ϕ and ψ hold in non-overlapping parts of the heap, that have disjoint domains. This connective allows for modular program analyses, because the formulæ specifying the behaviour of a program statement refer only to the small (local) set of locations that are manipulated by that statement, with no concern for the rest of the program's state.

Formulæ consisting of points-to atoms connected with separating conjunctions describe heaps of bounded size only. To reason about recursive data structures of unbounded sizes (lists, trees, etc.), the base logic is enriched by predicate symbols, with a semantics specified by user-defined inductive rules. For instance, the rules: $\mathsf{excls}(x,y) \Leftarrow \exists z \;.\; x \mapsto (z,y) * z \neq \mathsf{c}$ and $\mathsf{excls}(x,y) \Leftarrow \exists z \exists v \;.\; x \mapsto (z,v) * \mathsf{excls}(v,y) * z \neq \mathsf{c}$ describe a non-empty list segment, whose elements are records with two fields: the first is a data field, that keeps a list of locations, which excludes the location assigned to the

global constant c, and the second is used to link the records in a list whose head and tail are pointed to by x and y, respectively.

An important problem in program verification, arising during construction of Hoare-style correctness proofs, is the discharge of verification conditions, that are entailments of the form $\phi \vdash \psi_1, \ldots, \psi_n$, where ϕ and $\psi_1, \ldots, \psi_n$ are separating conjunctions of points-to, predicates and (dis-)equalities, also known as *symbolic heaps*. The *entailment problem* then asks if *every model of ϕ is a model of some ψ_i?* In general, the entailment problem is undecidable and becomes decidable when the inductive rules used to interpret the predicates satisfy three restrictions [8]: (1) *progress*, stating that each rule allocates *exactly* one memory cell, (2) *connectivity*, ensuring that the allocated memory cells form a tree-shaped structure, and (3) *establishment*, stating that all existentially quantified variables introduced by an inductive rule must be assigned to some allocated memory cell, in every structure defined by that rule. For instance, the above rules are progressing and connected but not established, because the $\exists z$ variables are not explicitly assigned an allocated location, unlike the $\exists v$ variables, passed as first parameter of the $\mathsf{excls}(x, y)$ predicate, and thus always allocated by the points-to atoms $x \mapsto (z, y)$ or $x \mapsto (z, v)$, from the first and second rule defining $\mathsf{excls}(x, y)$, respectively.

The argument behind the decidability of a progressing, connected and established entailment problem is that every model of the left-hand side is encoded by a graph whose treewidth[1] is bounded by the size of the largest symbolic heap that occurs in the problem [8]. Moreover, the progress and connectivity conditions ensure that the set of models of a symbolic heap can be represented by a Monadic Second Order (MSO) logic formula interpreted over graphs, that can be effectively built from the symbolic heap and the set of rules of the problem. The decidability of entailments follows then from the decidability of the satisfiability problem for MSO over graphs of bounded treewidth (Courcelle's Theorem) [4]. Initially, no upper bound better than elementary recursive was known to exist. Recently, a 2-EXPTIME algorithm was proposed [12, 14] for sets of rules satisfying these three conditions, and, moreover, this bound was shown to be tight [6].

Several natural questions arise: are the progress, connectivity and establishment conditions really necessary for the decidability of entailments? How much can these restriction be relaxed, without jeopardizing the complexity of the problem? Can one decide entailments that involve sets of heaps of unbounded treewidth? In this paper, we answer these questions by showing that entailments are still 2-EXPTIME-complete when the establishment condition is replaced by a condition on the (dis-)equations occurring in the symbolic heaps of the problem. Informally, such (dis-)equations must be of the form $x \doteq \mathsf{c}$ ($x \neq \mathsf{c}$), where c ranges over some finite and fixed set of globally visible constants (including special symbols such as nil, that denotes a non-allocated address, but also any free variable occurring on the left-hand side of the entailment). We also relax slightly the progress and connectivity conditions, by allowing forest-like heap structures (instead of just trees), provided that every root is mapped to a constant symbol. These entailment problems are called *equationally restricted* (*e-restricted*, for short). For instance, the entailment problem $\mathsf{excls}(x, y) * \mathsf{excls}(y, z) \vdash \mathsf{excls}(x, z)$, with the above rules, falls in this category.

We prove that the e-restricted condition loses no generality compared to establishment, because any established entailment problem can be transformed into an equivalent e-restricted entailment problem. E-restricted problems allow reasoning about structures that contain dangling pointers, which frequently occur in practice, especially in the context of modular program analysis. Moreover, the set of structures considered in an e-restricted entailment problem may contain infinite sequences of heaps of strictly increasing treewidths, that are out of the scope of established problems [8].

The decision procedure for e-restricted problems proposed in this paper is based on a similar idea as the one given, for established problems, in [14, 15]. We build a suitable abstraction of the set

[1] The treewidth of a graph is a parameter measuring how close the graph is to a tree, see [7, Ch. 11] for a definition.

of structures satisfying the left-hand side of the entailment bottom-up, starting from points-to and predicate atoms, using abstract operators to compose disjoint structures, to add and remove variables, and to unfold the inductive rules associated with the predicates. The abstraction is precise enough to allow checking that all the models of the left-hand side fulfill the right-hand side of the entailment and also general enough to ensure termination of the entailment checking algorithm.

Although both procedures are similar, there are essential differences between our work and [14, 15]. First, we show that instead of using a specific language for describing those abstractions, the considered set of structures can themselves be defined in SL, by means of formulæ of some specific pattern called *core formulæ*. Second, the fact that the systems are not established makes the definition of the procedure much more difficult, due to the fact that the considered structures can have an unbounded treewidth. This is problematic because, informally, this boundedness property is essential to ensure that the abstractions can be described using a finite set of variables, denoting the *frontier* of the considered structures, namely the locations that can be shared with other structures. In particular, the fact that disjoint heaps may share unallocated (or "unnamed") locations complexifies the definition of the composition operator. This problem is overcome by considering a specific class of structures, called *normal structures*, of bounded treewidth, and proving that the validity of an entailment can be decided by considering only normal structures.

In terms of complexity, we show that the running time of our algorithm is doubly exponential w.r.t. the maximal size among the symbolic heaps occurring in the input entailment problem (including those in the rules) and simply exponential w.r.t. the number of such symbolic heaps (hence w.r.t. the number of rules). This means that the 2-EXPTIME upper bound is preserved by any reduction increasing exponentially the number of rules, but increasing only polynomially the size of the rules. On the other hand, the 2-EXPTIME-hard lower bound is proved by a reduction from the membership problem for exponential-space bounded Alternating Turing Machines [6]. Due to space restrictions, most proofs are shifted to an appendix.

2 Separation Logic with Inductive Definitions

Let $\mathbb{N}$ denote the set of natural numbers. For a countable set S, we denote by $\|S\| \in \mathbb{N} \cup \{\infty\}$ its cardinality. For a partial mapping $f : A \rightharpoonup B$, let $\mathrm{dom}(f) \stackrel{\text{def}}{=} \{x \in A \mid f(x) \in B\}$ and $\mathrm{rng}(f) \stackrel{\text{def}}{=} \{f(x) \mid x \in \mathrm{dom}(f)\}$ be its domain and range, respectively. We say that f is *total* if $\mathrm{dom}(f) = A$, written $f : A \to B$ and *finite*, written $f : A \rightharpoonup_{fin} B$ if $\|\mathrm{dom}(f)\| < \infty$. Given integers n and m, we denote by $[\![n \,..\, m]\!]$ the set $\{n, n+1, \ldots, m\}$, so that $[\![n \,..\, m]\!] = \emptyset$ if $n > m$. For a relation $\lhd \subseteq A \times A$, we denote by $\lhd^*$ its reflexive and transitive closure.

For an integer $n \geq 0$, let A^n be the set of n-tuples with elements from A. Given a tuple $\mathbf{a} = (a_1, \ldots, a_n)$ and $i \in [\![1 \,..\, n]\!]$, we denote by $\mathbf{a}_i$ the i-th element of $\mathbf{a}$ and by $|\mathbf{a}| \stackrel{\text{def}}{=} n$ its length. By $f(\mathbf{a})$ we denote the tuple obtained by the pointwise application of f to the elements of $\mathbf{a}$. If multiplicity and order of the elements are not important, we blur the distinction between tuples and sets, using the set-theoretic notations $x \in \mathbf{a}$, $\mathbf{a} \cup \mathbf{b}$, $\mathbf{a} \cap \mathbf{b}$ and $\mathbf{a} \setminus \mathbf{b}$.

Let $\mathbb{V} = \{x, y, \ldots\}$ be an infinite countable set of logical first-order variables and $\mathbb{P} = \{p, q, \ldots\}$ be an infinite countable set (disjoint from $\mathbb{V}$) of relation symbols, called *predicates*, where each predicate p has arity $\#p \geq 0$. We also consider a finite set $\mathbb{C}$ of *constants*, of known bounded cardinality, disjoint from both $\mathbb{V}$ and $\mathbb{P}$. Constants will play a special rôle in the upcoming developments and the fact that $\mathbb{C}$ is bounded is of a particular importance. A *term* is either a variable or a constant and we denote by $\mathbb{T} \stackrel{\text{def}}{=} \mathbb{V} \cup \mathbb{C}$ the set of terms.

Throughout this paper we consider an integer $\mathfrak{K} \geq 1$ that, intuitively, denotes the number of fields in a record datatype. Although we do not assume $\mathfrak{K}$ to be a constant in any of the algorithms presented in the following, considering that every datatype has exactly $\mathfrak{K}$ records simplifies the definition. The

logic $\mathsf{SL}^{\mathfrak{K}}$ is the set of formulæ generated inductively by the syntax:

$$\phi \quad := \quad \mathsf{emp} \mid t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}}) \mid p(t_1, \ldots, t_{\#p}) \mid t_1 \approx t_2 \mid \phi_1 * \phi_2 \mid \phi_1 \wedge \phi_2 \mid \neg\phi_1 \mid \exists x \,.\, \phi_1$$

where $p \in \mathbb{P}$, $t_i \in \mathbb{T}$ and $x \in \mathbb{V}$. Atomic propositions of the form $t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}})$ are called *points-to atoms* and those of the form $p(t_1, \ldots, t_{\#p})$ are *predicate atoms*. If $\mathfrak{K} = 1$, we write $t_0 \mapsto t_1$ for $t_0 \mapsto (t_1)$.

The connective $*$ is called *separating conjunction*, in contrast with the classical conjunction $\wedge$. The *size* of a formula ϕ, denoted by $\mathrm{size}(\phi)$, is the number of occurrences of symbols in it. We write $\mathsf{fv}(\phi)$ for the set of *free* variables in ϕ and $\mathsf{trm}(\phi) \stackrel{\text{def}}{=} \mathsf{fv}(\phi) \cup \mathbb{C}$. A formula is *predicate-free* if it has no predicate atoms. As usual, $\phi_1 \vee \phi_2 \stackrel{\text{def}}{=} \neg(\neg\phi_1 \wedge \neg\phi_2)$ and $\forall x \,.\, \phi \stackrel{\text{def}}{=} \neg\exists x \,.\, \neg\phi$. For a set of variables $\mathbf{x} = \{x_1, \ldots, x_n\}$ and a quantifier $Q \in \{\exists, \forall\}$, we write $Q\mathbf{x} \,.\, \phi \stackrel{\text{def}}{=} Qx_1 \ldots Qx_n \,.\, \phi$. By writing $t_1 = t_2$ ($\phi_1 = \phi_2$) we mean that the terms (formulæ) t_1 and t_2 (ϕ_1 and ϕ_2) are syntactically the same.

A *substitution* is a partial mapping $\sigma : \mathbb{V} \rightharpoonup \mathbb{T}$ that maps variables to terms. We denote by $[t_1/x_1, \ldots, t_n/x_n]$ the substitution that maps the variable x_i to t_i, for each $i \in [\![1 \,..\, n]\!]$ and is undefined elsewhere. By $\phi\sigma$ we denote the formula obtained from ϕ by substituting each variable $x \in \mathsf{fv}(\phi)$ by $\sigma(x)$ (we assume that bound variables are renamed to avoid collisions if needed). By abuse of notation, we sometimes write $\sigma(x)$ for x, when $x \notin \mathrm{dom}(\sigma)$.

To interpret $\mathsf{SL}^{\mathfrak{K}}$ formulæ, we consider an infinite countable set $\mathbb{L}$ of *locations*. The semantics of $\mathsf{SL}^{\mathfrak{K}}$ formulæ is defined in terms of *structures* $(\mathfrak{s}, \mathfrak{h})$, where:

- $\mathfrak{s} : \mathbb{T} \rightharpoonup \mathbb{L}$ is a partial mapping of terms into locations, called a *store*, that interprets at least all the constants, i.e. $\mathbb{C} \subseteq \mathrm{dom}(\mathfrak{s})$ for every store $\mathfrak{s}$, and
- $\mathfrak{h} : \mathbb{L} \rightharpoonup_{fin} \mathbb{L}^{\mathfrak{K}}$ is a finite partial mapping of locations into $\mathfrak{K}$-tuples of locations, called a *heap*.

Given a heap $\mathfrak{h}$, let $\mathrm{loc}(\mathfrak{h}) \stackrel{\text{def}}{=} \{\ell_0, \ldots, \ell_{\mathfrak{K}} \mid \ell_0 \in \mathrm{dom}(\mathfrak{h}),\ \mathfrak{h}(\ell_0) = (\ell_1, \ldots, \ell_{\mathfrak{K}})\}$ be the set of locations that occur in the heap $\mathfrak{h}$. Two heaps $\mathfrak{h}_1$ and $\mathfrak{h}_2$ are *disjoint* iff $\mathrm{dom}(\mathfrak{h}_1) \cap \mathrm{dom}(\mathfrak{h}_2) = \emptyset$, in which case their *disjoint union* is denoted by $\mathfrak{h}_1 \uplus \mathfrak{h}_2$, otherwise undefined. The *frontier between* $\mathfrak{h}_1$ *and* $\mathfrak{h}_2$ is the set of common locations $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \stackrel{\text{def}}{=} \mathrm{loc}(\mathfrak{h}_1) \cap \mathrm{loc}(\mathfrak{h}_2)$. Note that disjoint heaps may have nonempty frontier. The *satisfaction relation* $\models$ between structures $(\mathfrak{s}, \mathfrak{h})$ and predicate-free $\mathsf{SL}^{\mathfrak{K}}$ formulæ ϕ is defined recursively on the structure of formulæ:

$$\begin{array}{lcll}
(\mathfrak{s},\mathfrak{h}) & \models & t_1 \approx t_2 & \Leftrightarrow \quad t_1, t_2 \in \mathrm{dom}(\mathfrak{s}) \text{ and } \mathfrak{s}(t_1) = \mathfrak{s}(t_2) \\
(\mathfrak{s},\mathfrak{h}) & \models & \mathsf{emp} & \Leftrightarrow \quad \mathfrak{h} = \emptyset \\
(\mathfrak{s},\mathfrak{h}) & \models & t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}}) & \Leftrightarrow \quad t_0, \ldots, t_{\mathfrak{K}} \in \mathrm{dom}(\mathfrak{s}),\ \mathrm{dom}(\mathfrak{h}) = \{\mathfrak{s}(t_0)\} \text{ and } \mathfrak{h}(\mathfrak{s}(t_0)) = (\mathfrak{s}(t_1), \ldots, \mathfrak{s}(t_{\mathfrak{K}})) \\
(\mathfrak{s},\mathfrak{h}) & \models & \phi_1 \wedge \phi_2 & \Leftrightarrow \quad (\mathfrak{s},\mathfrak{h}) \models \phi_i,\ i = 1,2 \\
(\mathfrak{s},\mathfrak{h}) & \models & \neg\phi_1 & \Leftrightarrow \quad \mathsf{fv}(\phi_1) \subseteq \mathrm{dom}(\mathfrak{s}) \text{ and } (\mathfrak{s},\mathfrak{h}) \not\models \phi_1 \\
(\mathfrak{s},\mathfrak{h}) & \models & \phi_1 * \phi_2 & \Leftrightarrow \quad \text{there exist heaps } \mathfrak{h}_1, \mathfrak{h}_2 \text{ such that } \mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2 \text{ and } (\mathfrak{s},\mathfrak{h}_i) \models \phi_i,\ i = 1,2 \\
(\mathfrak{s},\mathfrak{h}) & \models & \exists x \,.\, \phi & \Leftrightarrow \quad (\mathfrak{s}[x \leftarrow \ell], \mathfrak{h}) \models \phi, \text{ for some location } \ell \in \mathbb{L}
\end{array}$$

where $\mathfrak{s}[x \leftarrow \ell]$ is the store, with domain $\mathrm{dom}(\mathfrak{s}) \cup \{x\}$, that maps x to ℓ and behaves like $\mathfrak{s}$ over $\mathrm{dom}(\mathfrak{s}) \setminus \{x\}$. For a tuple of variables $\mathbf{x} = (x_1, \ldots, x_n)$ and locations $\overline{\ell} = (\ell_1, \ldots, \ell_n)$, we call the store $\mathfrak{s}[\mathbf{x} \leftarrow \overline{\ell}] \stackrel{\text{def}}{=} \mathfrak{s}[x_1 \leftarrow \ell_1] \ldots [x_n \leftarrow \ell_n]$ an $\mathbf{x}$-*associate* of $\mathfrak{s}$. A structure $(\mathfrak{s}, \mathfrak{h})$ such that $(\mathfrak{s}, \mathfrak{h}) \models \phi$, is called a *model* of ϕ. Note that $(\mathfrak{s}, \mathfrak{h}) \models \phi$ only if $\mathsf{fv}(\phi) \subseteq \mathrm{dom}(\mathfrak{s})$.

The fragment of *symbolic heaps* is obtained by confining the negation and conjunction to the formulæ $t_1 \doteq t_2 \stackrel{\text{def}}{=} t_1 \approx t_2 \wedge \mathsf{emp}$ and $t_1 \neq t_2 \stackrel{\text{def}}{=} \neg t_1 \approx t_2 \wedge \mathsf{emp}$, called *equational atoms*, by abuse of language. We denote by $\mathsf{SH}^{\mathfrak{K}}$ the set of symbolic heaps, formally defined below:

$$\phi \quad := \quad \mathsf{emp} \mid t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}}) \mid p(t_1, \ldots, t_{\#p}) \mid t_1 \doteq t_2 \mid t_1 \neq t_2 \mid \phi_1 * \phi_2 \mid \exists x \,.\, \phi_1$$

Given quantifier-free symbolic heaps $\phi_1, \phi_2 \in \mathsf{SH}^{\mathfrak{K}}$, it is not hard to check that $\exists x \,.\, \phi_1 * \exists y \,.\, \phi_2$ and $\exists x \exists y \,.\, \phi_1 * \phi_2$ have the same models. Consequently, each symbolic heap can be written in prenex form, as $\phi = \exists x_1 \ldots \exists x_n \,.\, \psi$, where ψ is a quantifier-free separating conjunction of points-to atoms and (dis-)equalities. A variable $x \in \mathsf{fv}(\psi)$ is *allocated* in ϕ iff there exists a (possibly empty) sequence of equalities $x \doteq \ldots \doteq t_0$ and a points-to atom $t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}})$ in ψ.

The predicates from $\mathbb{P}$ are intepreted by a given set $\mathcal{S}$ of *rules* $p(x_1,\ldots,x_{\#p}) \Leftarrow \rho$, where ρ is a symbolic heap, such that $\mathsf{fv}(\rho) \subseteq \{x_1,\ldots,x_{\#_p}\}$. We say that $p(x_1,\ldots,x_{\#p})$ is the *head* and ρ is the *body* of the rule. For conciseness, we write $p(x_1,\ldots,x_{\#p}) \Leftarrow_{\mathcal{S}} \rho$ instead of $p(x_1,\ldots,x_{\#p}) \Leftarrow \rho \in \mathcal{S}$. In the following, we shall often refer to a given set of rules $\mathcal{S}$.

▶ **Definition 1** (Unfolding). *A formula ψ is a* step-unfolding *of a formula $\phi \in \mathsf{SL}^{\mathfrak{K}}$, written $\phi \Rightarrow_{\mathcal{S}} \psi$, if ψ is obtained by replacing an occurrence of an atom $p(t_1,\ldots,t_{\#p})$ in ϕ with $\rho[t_1/x_1,\ldots,t_{\#p}/x_{\#p}]$, for a rule $p(x_1,\ldots,x_{\#p}) \Leftarrow_{\mathcal{S}} \rho$. An* unfolding *of ϕ is a formula ψ such that $\phi \Rightarrow^*_{\mathcal{S}} \psi$.*

It is easily seen that any unfolding of a symbolic heap is again a symbolic heap. We implicitly assume that all bound variables are α-renamed throughout an unfolding, to avoid name clashes. Unfolding extends the semantics from predicate-free to arbitrary $\mathsf{SL}^{\mathfrak{K}}$ formulæ:

▶ **Definition 2.** *Given a structure $(\mathfrak{s},\mathfrak{h})$ and a formula $\phi \in \mathsf{SL}^{\mathfrak{K}}$, we write $(\mathfrak{s},\mathfrak{h}) \models_{\mathcal{S}} \phi$ iff there exists a predicate-free unfolding $\phi \Rightarrow^*_{\mathcal{S}} \psi$ such that $(\mathfrak{s},\mathfrak{h}) \models \psi$. In this case, $(\mathfrak{s},\mathfrak{h})$ is an $\mathcal{S}$-*model of ϕ. *For two formulæ $\phi,\psi \in \mathsf{SL}^{\mathfrak{K}}$, we write $\phi \models_{\mathcal{S}} \psi$ iff every $\mathcal{S}$-model of ϕ is an $\mathcal{S}$-model of ψ.*

Note that, if $(\mathfrak{s},\mathfrak{h}) \models_{\mathcal{S}} \phi$, then $\mathrm{dom}(\mathfrak{s})$ might have to contain constants that do not occur in ϕ. For instance if $p(x) \Leftarrow_{\mathcal{S}} x \mapsto \mathsf{a}$ is the only rule with head $p(x)$, then any $\mathcal{S}$-model $(\mathfrak{s},\mathfrak{h})$ must map a to some location, which is taken care of by the assumption $\mathbb{C} \subseteq \mathrm{dom}(\mathfrak{s})$, that applies to any store.

▶ **Definition 3** (Entailment). *Given symbolic heaps $\phi,\psi_1,\ldots,\psi_n$, such that ϕ is quantifier-free and $\mathsf{fv}(\phi) = \mathsf{fv}(\psi_1) = \ldots = \mathsf{fv}(\psi_n) = \emptyset$, the* sequent $\phi \vdash \psi_1,\ldots,\psi_n$ *is* valid for $\mathcal{S}$ *iff $\phi \models_{\mathcal{S}} \bigvee_{i=1}^{n} \phi_i$. An* entailment problem $\mathcal{P} = (\mathcal{S},\Sigma)$ *consists of a set of rules $\mathcal{S}$ and a set Σ of sequents, asking whether each sequent in Σ is valid for $\mathcal{S}$.*

Note that we consider entailments between formulæ without free variables. This is not restrictive, since any free variable can be replaced by a constant from $\mathbb{C}$, with no impact on the validity status or the computational complexity of the problem. We silently assume that $\mathbb{C}$ contains enough constants to allow this replacement. For conciseness, we write $\phi \vdash_{\mathcal{P}} \psi_1,\ldots,\psi_n$ for $\phi \vdash \psi_1,\ldots,\psi_n \in \Sigma$, where Σ is the set of sequents of $\mathcal{P}$. The following example shows an entailment problem asking whether the concatenation of two acyclic lists is again an acyclic list:

▶ **Example 4.** The entailment problem below consists of four rules, defining the predicates $\mathsf{ls}(x,y)$ and $\mathsf{sls}(x,y,z)$, respectively, and two sequents:

$$\begin{array}{rcl} \mathsf{ls}(x,y) & \Leftarrow & x \mapsto y * x \neq y \mid \exists v \,.\, x \mapsto v * \mathsf{ls}(v,y) * x \neq y \\ \mathsf{sls}(x,y,z) & \Leftarrow & x \mapsto y * x \neq y * x \neq z \mid \exists v \,.\, x \mapsto v * \mathsf{sls}(v,y,z) * x \neq y * x \neq z \\ \mathsf{ls}(a,b) * \mathsf{ls}(b,c) & \vdash & \exists x \,.\, a \mapsto x * \mathsf{ls}(x,c) * a \neq c \qquad \mathsf{sls}(a,b,c) * \mathsf{ls}(b,c) \vdash \exists x \,.\, a \mapsto x * \mathsf{ls}(x,c) * a \neq c \end{array}$$

Here $\mathsf{ls}(x,y)$ describes non-empty acyclic list segments with head and tail pointed to by x and y, respectively. The first sequent is invalid, because c can be allocated within the list segment defined by $\mathsf{ls}(a,b)$, in which case the entire list has a cycle starting and ending with the location associated with c. To avoid the cycle, the left-hand side of the second sequent uses the predicate $\mathsf{sls}(x,y,z)$ describing an acyclic list segment from x to y that skips the location pointed to by z. The second sequent is valid. ■

The complexity analysis of the decision procedure described in this paper relies on two parameters. First, the *width* of an entailment problem $\mathcal{P} = (\mathcal{S},\Sigma)$ is (roughly) the maximum among the sizes of the symbolic heaps occurring in $\mathcal{P}$ and the number of constants in $\mathbb{C}$. Second, the *size* of the entailment problem is (roughly) the number of symbols needed to represent it, namely:

$$\begin{array}{rcl} \mathrm{width}(\mathcal{P}) & \stackrel{\mathrm{def}}{=} & \max\left(\{\mathrm{size}(\rho) + \#p \mid p(x_1,\ldots,x_{\#p}) \Leftarrow_{\mathcal{S}} \rho\} \cup \{\mathrm{size}(\psi_i) \mid \psi_0 \vdash_{\mathcal{P}} \psi_1,\ldots,\psi_n\} \cup \{\|\mathbb{C}\|\}\right) \\ \mathrm{size}(\mathcal{P}) & \stackrel{\mathrm{def}}{=} & \sum_{p(x_1,\ldots,x_{\#p}) \Leftarrow_{\mathcal{S}} \rho} (\mathrm{size}(\rho) + \#p) + \sum_{\psi_0 \vdash_{\mathcal{P}} \psi_1,\ldots,\psi_n} \sum_{i=1}^{n} \mathrm{size}(\psi_i) \end{array}$$

In the next section we give a transformation of an entailment problems with a time complexity that is bounded by the product of the size and a simple exponential of the width of the input, such that,

moreover, the width of the problem increases by a polynomial factor only. The latter is instrumental in proving the final 2-EXPTIME upper bound on the complexity of the entailment problem.

To alleviate the upcoming technical details, we make the following assumption:

▶ **Assumption 1.** *Distinct constants are always associated with distinct locations: for all stores* $\mathfrak{s}$*, and for all* $c, d \in \mathbb{C}$*, we have* $c \neq d$ *only if* $\mathfrak{s}(c) \neq \mathfrak{s}(d)$*.*

This assumption loses no generality, because one can enumerate all the equivalence relations on $\mathbb{C}$ and test the entailments separately for each of these relations, by replacing all the constants in the same class by a unique representative[2], while assuming that constants in distinct classes are mapped to distinct locations. The overall complexity of the procedure is still doubly exponential, since the number of such equivalence relations is bounded by the number of partitions of $\mathbb{C}$, that is $2^{O(\|\mathbb{C}\| \cdot \log \|\mathbb{C}\|)} = 2^{O(\|\mathsf{width}(\mathcal{P})\| \cdot \log \|\mathsf{width}(\mathcal{P})\|)}$, for any entailment problem $\mathcal{P}$. Thanks to Assumption 1, the considered symbolic heaps can be, moreover, safely assumed not to contain atoms $c \bowtie d$, with $\bowtie \in \{\doteq, \not\doteq\}$ and $c, d \in \mathbb{C}$, since these atoms are either unsatisfiable or equivalent to emp.

3 Decidable Classes of Entailments

In general, the entailment problem (Definition 3) is undecidable and we refer the reader to [9, 1] for two different proofs. A first attempt to define a naturally expressive class of formulæ with a decidable entailment problem was reported in [8]. The entailments considered in [8] involve sets of rules restricted by three conditions, recalled below, in a slightly generalized form.

First, the *progress* condition requires that each rule adds to the heap exactly one location, associated either to a constant or to a designated parameter. Formally, we consider a mapping $\mathsf{root} : \mathbb{P} \to \mathbb{N} \cup \mathbb{C}$, such that $\mathsf{root}(p) \in [\![1 \,..\, \#p]\!] \cup \mathbb{C}$, for each $p \in \mathbb{P}$. The term $\mathsf{root}(p(t_1, \ldots, t_{\#p}))$ denotes either t_i if $\mathsf{root}(p) = i \in [\![1 \,..\, \#p]\!]$, or the constant $\mathsf{root}(p)$ itself if $\mathsf{root}(p) \in \mathbb{C}$. The notation $\mathsf{root}(\alpha)$ is extended to points-to atoms α as $\mathsf{root}(t_0 \mapsto (t_1, \ldots, t_\mathfrak{K})) \stackrel{\text{def}}{=} t_0$. Second, the *connectivity* condition requires that all locations added during an unfolding of a predicate atom form a set of connected trees (a forest) rooted in locations associated either with a parameter of the predicate or with a constant.

▶ **Definition 5** (Progress & Connectivity)**.** *A set of rules* $\mathcal{S}$ *is* progressing *if each rule in* $\mathcal{S}$ *is of the form* $p(x_1, \ldots, x_{\#p}) \Leftarrow \exists z_1 \ldots \exists z_m \,.\, \mathsf{root}(p(x_1, \ldots, x_{\#p})) \mapsto (t_1, \ldots, t_\mathfrak{K}) * \psi$ *and* ψ *contains no occurrences of points-to atoms. Moreover,* $\mathcal{S}$ *is* connected *if* $\mathsf{root}(q(u_1, \ldots, u_{\#q})) \in \{t_1, \ldots, t_\mathfrak{K}\} \cup \mathbb{C}$*, for each predicate atom* $q(u_1, \ldots, u_{\#q})$ *occurring in* ψ*. An entailment problem* $\mathcal{P} = (\mathcal{S}, \Sigma)$ *is progressing (connected) if* $\mathcal{S}$ *is progressing (connected).*

The progress and connectivity conditions can be checked in polynomial time by a syntactic inspection of the rules in $\mathcal{S}$, even if the $\mathsf{root}(.)$ function is not known à priori. Note that this definition of connectivity is less restrictive that the definition from [8], that asked for $\mathsf{root}(q(u_1, \ldots, u_{\#q})) \in \{t_1, \ldots, t_\mathfrak{K}\}$. For instance, the set of rules $\{\mathsf{p}(x) \Leftarrow \exists y \,.\, x \mapsto y * \mathsf{p}(y) * \mathsf{p}(\mathsf{c}), \mathsf{p}(x) \Leftarrow x \mapsto \mathsf{nil}\}$, where $\mathsf{c} \in \mathbb{C}$ is progressing and connected (with $\mathsf{root}(\mathsf{p}) = 1$) in the sense of Definition 5, but not connected in the sense of [8], because $\mathsf{c} \notin (y)$. Note also that nullary predicate symbols are allowed, for instance $\mathsf{q}() \Leftarrow \mathsf{c} \mapsto \mathsf{nil}$ is progressing and connected (with $\mathsf{root}(\mathsf{q}) = \mathsf{c}$). Further, the entailment problem from Example 4 is both progressing and connected.

Third, the *establishment* condition is defined, slightly extended from its original statement [8]:

[2] The replacement must be performed also within the inductive rules, not only in the considered formulæ.

▶ **Definition 6** (Establishment). *Given a set of rules $\mathcal{S}$, a symbolic heap $\exists x_1 \ldots \exists x_n \,.\, \phi$, where ϕ is quantifier-free, is* $\mathcal{S}$-established *iff every x_i for $i \in [\![1 \,..\, n]\!]$ is allocated in each predicate-free unfolding $\phi \Rightarrow^*_{\mathcal{S}} \varphi$. A set of rules $\mathcal{S}$ is* established *if the body ρ of each rule $p(x_1, \ldots, x_{\#p}) \Leftarrow_{\mathcal{S}} \rho$ is $\mathcal{S}$-established. An entailment problem $\mathcal{P} = (\mathcal{S}, \Sigma)$ is established if $\mathcal{S}$ is established, and* strongly established *if, moreover, ϕ_i is $\mathcal{S}$-established, for each sequent $\phi_0 \vdash_{\mathcal{P}} \phi_1, \ldots, \phi_n$ and each $i \in [\![0 \,..\, n]\!]$.*

For example, the entailment problem from Example 4 is strongly established.

In this paper, we replace establishment with a new condition that, as we show, preserves the decidability and computational complexity of progressing, connected and established entailment problems. The new condition can be checked in time linear in the size of the problem. This condition, called *equational restrictedness* (*e-restrictedness*, for short), requires that each equational atom occurring in a formula involves at least one constant. We will show that the e-restrictedness condition is more general than establishment, in the sense that every established problem can be reduced to an equivalent e-restricted problem (Theorem 13). Moreover, the class of structures defined using e-restricted symbolic heaps is a strict superset of the one defined by established symbolic heaps.

▶ **Definition 7** (E-restrictedness). *A symbolic heap ϕ is* e-restricted *if, for every equational atom $t \bowtie u$ from ϕ, where $\bowtie \in \{\doteq, \neq\}$, we have $\{t, u\} \cap \mathbb{C} \neq \emptyset$. A set of rules $\mathcal{S}$ is* e-restricted *if the body ρ of each rule $p(x_1, \ldots, x_{\#p}) \Leftarrow_{\mathcal{S}} \rho$ is e-restricted. An entailment problem $\mathcal{P} = (\mathcal{S}, \Sigma)$ is* e-restricted *if $\mathcal{S}$ is e-restricted and ϕ_i is e-restricted, for each sequent $\phi_0 \vdash_{\mathcal{P}} \phi_1, \ldots, \phi_n$ and each $i \in [\![0 \,..\, n]\!]$.*

For instance, the entailment problem from Example 4 is not e-restricted, because several rule bodies have disequalities between parameters, e.g. $\mathsf{ls}(x, y) \Leftarrow x \mapsto y * x \neq y$. However, the set of rules $\{\mathsf{ls}_{\mathsf{c}}(x) \Leftarrow x \mapsto c * x \neq \mathsf{c}, \mathsf{ls}_{\mathsf{c}}(x) \Leftarrow \exists y \,.\, x \mapsto y * \mathsf{ls}_{\mathsf{c}}(y) * x \neq \mathsf{c}\}$, where $\mathsf{c} \in \mathbb{C}$ and ls_{c} is a new predicate symbol, denoting an acyclic list ending with c, is e-restricted. Note that any atom $\mathsf{ls}(x, y)$ can be replaced by $\mathsf{ls}_{\mathsf{y}}(x)$, provided that y occurs free in a sequent and can be viewed as a constant.

We show next that every established entailment problem (Definition 6) can be reduced to an e-restricted entailment problem (Definition 7). The transformation incurs an exponential blowup, however, as we show, the blowup is exponential only in the width and polynomial in the size of the input problem. This is to be expected, because checking e-restrictedness of a problem can be done in linear time, in contrast with checking establishment, which is at least co-NP-hard [11].

We begin by showing that each problem can be translated into an equivalent *normalized* problem:

▶ **Definition 8** (Normalization).

(1) A symbolic heap $\exists \mathbf{x} \,.\, \psi \in \mathsf{SH}^{\mathfrak{R}}$, where ψ is quantifier-free, is normalized *iff for every atom α in ψ:*
   a. if α is an equational atom, then it is of the form $x \neq t$ ($t \neq x$), where $x \in \mathbf{x}$,
   b. every variable $x \in \mathsf{fv}(\psi)$ occurs in a points-to or predicate atom of ψ,
   c. if α is a predicate atom $q(t_1, \ldots, t_{\#q})$, then $\{t_1, \ldots, t_{\#q}\} \cap \mathbb{C} = \emptyset$ and $t_i \neq t_j$, for all $i \neq j \in [\![1 \,..\, \#q]\!]$.

(2) A set of rules $\mathcal{S}$ is normalized *iff for each rule $p(x_1, \ldots, x_{\#p}) \Leftarrow_{\mathcal{S}} \rho$, the symbolic heap ρ is normalized and, moreover:*
   a. For every $i \in [\![1 \,..\, \#p]\!]$ and every predicate-free unfolding $p(x_1, \ldots, x_{\#p}) \Rightarrow^*_{\mathcal{S}} \varphi$, φ contains a points-to atom $t_0 \mapsto (t_1, \ldots, t_{\mathfrak{R}})$, such that $x_i \in \{t_0, \ldots, t_{\mathfrak{R}}\}$.
   b. There exist sets $\mathsf{palloc}_{\mathcal{S}}(p) \subseteq [\![1 \,..\, \#p]\!]$ and $\mathsf{calloc}_{\mathcal{S}}(p) \subseteq \mathbb{C}$ such that, for each predicate-free unfolding $p(x_1, \ldots, x_{\#p}) \Rightarrow^*_{\mathcal{S}} \varphi$:
      - *$i \in \mathsf{palloc}_{\mathcal{S}}(p)$ iff φ contains an atom $x_i \mapsto (t_1, \ldots, t_{\mathfrak{R}})$, for every $i \in [\![1 \,..\, \#p]\!]$,*
      - *$c \in \mathsf{calloc}_{\mathcal{S}}(p)$ iff φ contains an atom $c \mapsto (t_1, \ldots, t_{\mathfrak{R}})$, for every $c \in \mathbb{C}$.*
   c. For every predicate-free unfolding $p(x_1, \ldots, x_{\#p}) \Rightarrow^*_{\mathcal{S}} \varphi$, if φ contains an atom $t_0 \mapsto (t_1, \ldots, t_{\mathfrak{R}})$ such that $t_0 \in \mathbb{V} \setminus \{x_1, \ldots, x_{\#p}\}$, then φ also contains atoms $t_0 \neq c$, for every $c \in \mathbb{C}$.

(3) An entailment problem $\mathcal{P} = (\mathcal{S}, \Sigma)$ is normalized *if $\mathcal{S}$ is normalized and, for each sequent $\phi_0 \vdash_{\mathcal{P}} \phi_1, \ldots, \phi_n$ the symbolic heap ϕ_i is normalized, for each $i \in [\![0 \,..\, n]\!]$.*

The intuition behind Condition (2a) is that no term can "disappear" while unfolding an inductive definition. Condition (2b) states that the set of terms eventually allocated by a predicate atom is the same in all unfoldings. This allows to define the set of symbols that occur freely in a symbolic heap ϕ and are necessarily allocated in every unfolding of ϕ, provided that the set of rules is normalized:

▶ **Definition 9.** *Given a normalized set of rules $\mathcal{S}$ and a symbolic heap $\phi \in \mathsf{SH}^{\mathfrak{R}}$, the set* $\mathsf{alloc}_{\mathcal{S}}(\phi)$ *is defined recursively on the structure of ϕ:*

$$\begin{array}{rcl@{\qquad}rcl}
\mathsf{alloc}_{\mathcal{S}}(t_0 \mapsto (t_1,\ldots,t_{\mathfrak{R}})) & \stackrel{\text{def}}{=} & \{t_0\} & \mathsf{alloc}_{\mathcal{S}}(p(t_1,\ldots,t_{\#p})) & \stackrel{\text{def}}{=} & \{t_i \mid i \in \mathsf{palloc}_{\mathcal{S}}(p)\} \\
\mathsf{alloc}_{\mathcal{S}}(t_1 \bowtie t_2) & \stackrel{\text{def}}{=} & \emptyset,\ \bowtie \in \{\doteq, \neq\} & & & \cup\ \mathsf{calloc}_{\mathcal{S}}(p) \\
\mathsf{alloc}_{\mathcal{S}}(\phi_1 * \phi_2) & \stackrel{\text{def}}{=} & \mathsf{alloc}_{\mathcal{S}}(\phi_1) \cup \mathsf{alloc}_{\mathcal{S}}(\phi_2) & \mathsf{alloc}_{\mathcal{S}}(\exists x\ .\ \phi_1) & \stackrel{\text{def}}{=} & \mathsf{alloc}_{\mathcal{S}}(\phi_1) \setminus \{x\}
\end{array}$$

▶ **Example 10.** The rules $p(x,y) \Leftarrow \exists z\ .\ x \mapsto z * p(z,y) * x \neq y$ and $p(x,y) \Leftarrow \exists z\ .\ x \mapsto z$ are not normalized, because they contradict Conditions (1a) and (2a) of Definition 8, respectively. A set $\mathcal{S}$ containing the rules $q(x,y) \Leftarrow \exists z\ .\ x \mapsto y * q(y,z)$ and $q(x,y) \Leftarrow x \mapsto y$ is not normalized, because it is not possible to find a set $\mathsf{palloc}_{\mathcal{S}}(q)$ satisfying Condition (2b). Indeed, if $2 \in \mathsf{palloc}_{\mathcal{S}}(q)$ then the required equivalence does not hold for the second rule (because it does not allocate y), and if $2 \notin \mathsf{palloc}_{\mathcal{S}}(q)$ then it fails for the first one (since the predicate $q(y,z)$ allocates y). On the other hand, $\mathcal{S}' = \{p(x,y) \Leftarrow \exists z\ .\ x \mapsto z * p(z,y) * z \neq x * z \neq \mathsf{nil}, p(x,y) \Leftarrow x \mapsto y, q(x,y) \Leftarrow \exists z\ .\ x \mapsto y * q(y,z) * z \neq \mathsf{nil}\ ,\ q(x,y) \Leftarrow x \mapsto y * r(y), r(x) \Leftarrow x \mapsto \mathsf{nil}\}$ is normalized (assuming $\mathbb{C} = \{\mathsf{nil}\}$), with $\mathsf{palloc}_{\mathcal{S}'}(p) = \mathsf{palloc}_{\mathcal{S}'}(r) = \{1\}$, $\mathsf{palloc}_{\mathcal{S}'}(q) = \{1,2\}$ and $\mathsf{calloc}_{\mathcal{S}'}(\pi) = \emptyset$, for all $\pi \in \{p,q,r\}$. Then $\mathsf{alloc}_{\mathcal{S}'}(p(x_1,x_2) * q(x_3,x_4) * r(x_5)) = \{x_1,x_3,x_4,x_5\}$. ■

The following lemma states that every entailment problem can be transformed into a normalized entailment problem, by a transformation that preserves e-restricted-ness and (strong) establishment.

▶ **Lemma 11.** *An entailment problem $\mathcal{P}$ can be translated to an equivalent normalized problem $\mathcal{P}_n$, such that* $\mathrm{width}(\mathcal{P}_n) = O(\mathrm{width}(\mathcal{P})^2)$ *in time* $\mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$*. Further, $\mathcal{P}_n$ is e-restricted and (strongly) established if $\mathcal{P}$ is e-restricted and (strongly) established.*

▶ **Example 12.** The entailment problem $\mathcal{P} = (\mathcal{S}, \{p(\mathsf{a},\mathsf{b}) \vdash \exists x,y\ .\ q(x,y)\})$ with:

$$\mathcal{S} \stackrel{\text{def}}{=} \left\{ \begin{array}{rcl@{\qquad}rcl}
p(x,y) & \Leftarrow & \exists z\ .\ x \mapsto z * p(z,y) * x \neq y & q(x,y) & \Leftarrow & \exists z\ .\ x \mapsto y * q(y,z) * z \neq \mathsf{a} * z \neq \mathsf{b} \\
p(x,y) & \Leftarrow & \exists z\ .\ x \mapsto z & q(x,y) & \Leftarrow & x \mapsto y
\end{array} \right\}$$

may be transformed into $(\mathcal{S}', \{p_1() \vdash \exists x,y\ .\ q_1(x,y), \exists x,y\ .\ q_2(x,y)\})$, where:

$$\mathcal{S}' \stackrel{\text{def}}{=} \left\{ \begin{array}{rcl@{\qquad}rcl}
p_1() & \Leftarrow & \exists z\ .\ \mathsf{a} \mapsto z * p_2(z) * z \neq \mathsf{a} * z \neq \mathsf{b} & p_1() & \Leftarrow & \mathsf{a} \mapsto \mathsf{b} * p_3() \\
p_1() & \Leftarrow & \exists z\ .\ \mathsf{a} \mapsto z & p_2(x) & \Leftarrow & x \mapsto \mathsf{b} * p_3() \\
p_2(x) & \Leftarrow & \exists z\ .\ x \mapsto z * p_2(z) * z \neq \mathsf{a} * z \neq \mathsf{b} & p_2(x) & \Leftarrow & \exists z\ .\ x \mapsto z \\
p_3() & \Leftarrow & \exists z\ .\ \mathsf{b} \mapsto z & q_1(x,y) & \Leftarrow & \exists z\ .\ x \mapsto y * q_1(y,z) * z \neq \mathsf{a} * z \neq \mathsf{b} \\
q_1(x,y) & \Leftarrow & \exists z\ .\ x \mapsto y * q_2(y,z) * z \neq \mathsf{a} * z \neq \mathsf{b} & q_2(x,y) & \Leftarrow & x \mapsto y
\end{array} \right\}$$

The predicate atoms $p_1(), p_2(x)$ and $p_3()$ are equivalent to $p(\mathsf{a},\mathsf{b})$, $p(x,\mathsf{b})$ and $p(\mathsf{b},\mathsf{b})$, respectively. $q(x,y)$ is equivalent to $q_1(x,y) \vee q_2(x,y)$. Note that $p_2(x)$ is only used in a context where $x \neq b$ holds, thus this atom may be omitted from the rules of $p_2()$. Recall that a and b are mapped to distinct locations, by Assumption 1. ■

We show that every established problem $\mathcal{P}$ can be reduced to an e-restricted problem in time linear in the size and exponential in the width of the input, at the cost of a polynomial increase of its width:

▶ **Theorem 13.** *Every established entailment problem $\mathcal{P} = (\mathcal{S}, \Sigma)$ can be reduced in time* $\mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$ *to normalized an e-restricted problem $\mathcal{P}_r$, such that* $\mathrm{width}(\mathcal{P}_r) = O(\mathrm{width}(\mathcal{P}))$.

The class of e-restricted problems is more general than the class of established problems, in the following sense: for each established problem $\mathcal{P} = (\mathcal{S}, \Sigma)$, the treewidth of each $\mathcal{S}$-model of a $\mathcal{S}$-established symbolic heap ϕ is bounded by $\mathrm{width}(\mathcal{P})$ [8], while e-restricted symbolic heaps may have infinite sequences of models with strictly increasing treewidth:

▶ **Example 14.** Consider the set of rules $\{\mathsf{lls}(x,y) \Leftarrow x \mapsto (y,\mathsf{nil}),\ \mathsf{lls}(x,y) \Leftarrow \exists z \exists v\ .\ x \mapsto (z,v) * \mathsf{lls}(z,y)\}$. The existentially quantified variable v in the second rule in never allocated in any predicate-free unfolding of $\mathsf{lls}(\mathsf{a},\mathsf{b})$, thus the set of rules is not established. However, it is trivially e-restricted, because no equational atoms occur within the rules. Among the models of $\mathsf{lls}(\mathsf{a},\mathsf{b})$, there are all $n \times n$-square grid structures, known to have treewidth n, for $n > 1$ [17]. ■

4 Normal Structures

The decidability of e-restricted entailment problems relies on the fact that, to prove the validity of a sequent, it is sufficient to consider only a certain class of structures, called *normal*, that require the variables not mapped to the same location as a constant to be mapped to pairwise distinct locations:

▶ **Definition 15.** *A structure* $(\mathfrak{s},\mathfrak{h})$ *is a* normal $\mathcal{S}$-model *of a symbolic heap* ϕ *iff there exists:*

1. *a predicate-free unfolding* $\phi \Rightarrow_{\mathcal{S}} \exists \mathbf{x}\ .\ \psi$*, where* ψ *is quantifier-free, and*
2. *an* $\mathbf{x}$*-associate* $\overline{\mathfrak{s}}$ *of* $\mathfrak{s}$*, such that* $(\overline{\mathfrak{s}},\mathfrak{h}) \models_{\mathcal{S}} \psi$ *and* $\overline{\mathfrak{s}}(x) = \overline{\mathfrak{s}}(y) \wedge x \neq y \Rightarrow \overline{\mathfrak{s}}(x) \in \mathfrak{s}(\mathbb{C})$*, for all* $x, y \in \mathsf{fv}(\psi)$*.*

▶ **Example 16.** Consider the formula $\varphi = p(x_1) * p(x_2)$, with $p(x) \Leftarrow_{\mathcal{S}} \exists z\ .\ x \mapsto z$ and $\mathbb{C} = \{\mathsf{a}\}$. Then the structures: $(\mathfrak{s},\mathfrak{h})$ and $(\mathfrak{s},\mathfrak{h}')$ with $\mathfrak{s} = \{(x_1,\ell_1),(x_2,\ell_2),(\mathsf{a},\ell_3)\}$, $\mathfrak{h} = \{(\ell_1,\ell_3),(\ell_2,\ell_3)\}$ and $\mathfrak{h}' = \{(\ell_1,\ell_4),(\ell_2,\ell_5)\}$ are normal models of φ. On the other hand, if $\mathfrak{h}'' = \{(\ell_1,\ell_4),(\ell_2,\ell_4)\}$ (with $\ell_4 \neq \ell_3$) then $(\mathfrak{s},\mathfrak{h}'')$ is a model of φ but it is not normal, because any associate of $\mathfrak{s}$ will map the existentials from the predicate-free unfolding of $p(x_1) * p(x_2)$ into the same location, different from $\mathfrak{s}(\mathsf{a})$. ■

Since the left-hand side symbolic heap ϕ of each sequent $\phi \vdash \psi_1,\ldots,\psi_n$ is quantifier-free and has no free variables (Definition 3) and moreover, by Assumption 1, every constant is associated a distinct location, to check the validity of a sequent it is enough to consider only structures with injective stores. We say that a structure $(\dot{\mathfrak{s}},\mathfrak{h})$ is *injective* if the store $\dot{\mathfrak{s}}$ is injective. As a syntactic convention, by stacking a dot on the symbol denoting the store, we mean that the store is injective.

The key property of normal structures is that validity of e-restricted entailment problems can be checked considering only (injective) normal structures. The intuition is that, since the (dis-)equalities occurring in the considered formula involve a constant, it is sufficient to assume that all the existential variables not equal to a constant are mapped to pairwise distinct locations, as all other structures can be obtained from such structures by applying a morphism that preserves the truth value of the considered formulæ[3].

▶ **Lemma 17.** *Let* $\mathcal{P} = (\mathcal{S},\Sigma)$ *be a normalized and e-restricted entailment problem and let* $\phi \vdash_{\mathcal{P}} \psi_1,\ldots,\psi_n$ *be a sequent. Then* $\phi \vdash_{\mathcal{P}} \psi_1,\ldots,\psi_n$ *is valid for* $\mathcal{S}$ *iff* $(\dot{\mathfrak{s}},\mathfrak{h}) \models_{\mathcal{S}} \bigvee_{i=1}^{n} \psi_i$*, for each normal injective* $\mathcal{S}$*-model* $(\dot{\mathfrak{s}},\mathfrak{h})$ *of* ϕ*.*

Another important property of injective normal structures is that the frontier $\mathrm{Fr}(\mathfrak{h}_1,\mathfrak{h}_2)$ of a heap decomposition $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$ such that $(\dot{\mathfrak{s}},\mathfrak{h}) \models_{\mathcal{S}} \phi_1 * \phi_2$ and $(\dot{\mathfrak{s}},\mathfrak{h}_i) \models_{\mathcal{S}} \phi_i$, for each $i = 1,2$ is contained in the image of the common free variables and constants via $\mathfrak{s}$, i.e. $\mathrm{Fr}(\mathfrak{h}_1,\mathfrak{h}_2) \subseteq \dot{\mathfrak{s}}(\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C})$[4].

5 Core Formulæ

Given an e-restricted entailment problem $\mathcal{P} = (\mathcal{S},\Sigma)$, the idea of the entailment checking algorithm is to compute, for each symbolic heap ϕ that occurs as the left-hand side of a sequent $\phi \vdash_{\mathcal{P}} \psi_1,\ldots,\psi_n$, a finite set of sets of formulæ $\mathcal{F}(\phi) = \{F_1,\ldots,F_m\}$, of some specific pattern, called *core formulæ*. The

[3] See Appendices D and E for more details.
[4] See Lemma 36 in Appendix D for details.

set $\mathcal{F}(\phi)$ defines an equivalence relation, of finite index, on the set of injective normal $\mathcal{S}$-models of ϕ, such that each set $F \in \mathcal{F}(\phi)$ encodes an equivalence class. Because the validity of each sequent can be checked by testing whether every (injective) normal model of its left-hand side is a model of some symbolic heap on the right-hand side (Lemma 17), an equivalent check is that each set $F \in \mathcal{F}(\phi)$ contains a core formula entailing some formula ψ_i, for $i = 1, \ldots, n$. To improve the presentation, we first formalize the notions of core formulæ and abstractions by sets of core formulæ, while deferring the effective construction of $\mathcal{F}(\phi)$, for a symbolic heap ϕ, to the next section (§6). In the following, we refer to a given entailment problem $\mathcal{P} = (\mathcal{S}, \Sigma)$.

First, we define core formulæ as a fragment of $\mathsf{SL}^{\Re}$. Consider the formula $\mathsf{loc}(x) \stackrel{\text{def}}{=} \exists y_0 \ldots \exists y_{\Re} \,.\, y_0 \mapsto (y_1, \ldots, y_{\Re}) * \bigvee_{i=0}^{\Re} x \approx y_i$. Note that a structure is a model of $\mathsf{loc}(x)$ iff the variable x is assigned to a location from the domain or the range of the heap. We define also the following bounded quantifiers:

$$\dot{\exists} x \,.\, \phi \stackrel{\text{def}}{=} \exists x \,.\, \bigwedge_{t \in (\mathsf{fv}(\phi) \setminus \{x\}) \cup \mathbb{C}} \neg x \approx t \wedge \phi \qquad \exists_{\mathsf{h}} x \,.\, \phi \stackrel{\text{def}}{=} \dot{\exists} x \,.\, \mathsf{loc}(x) \wedge \phi$$
$$\exists_{\neg \mathsf{h}} x \,.\, \phi \stackrel{\text{def}}{=} \dot{\exists} x \,.\, \neg \mathsf{loc}(x) \wedge \phi \qquad \forall_{\neg \mathsf{h}} x \,.\, \phi \stackrel{\text{def}}{=} \neg \exists_{\neg \mathsf{h}} x \,.\, \neg \phi$$

In the following, we shall be extensively using the $\exists_{\mathsf{h}} x \,.\, \phi$ and $\forall_{\neg \mathsf{h}} x \,.\, \phi$ quantifiers. The formula $\exists_{\mathsf{h}} x \,.\, \phi$ states that there exists a location ℓ which occurs in the domain or range of the heap and is distinct from the locations associated with the constants and free variables, such that ϕ holds when x is associated with ℓ. Similarly, $\forall_{\neg \mathsf{h}} x \,.\, \phi$ states that ϕ holds if x is associated with any location ℓ that is outside of the heap and distinct from all the constants and free variables. The use of these special quantifiers will allow us to restrict ourselves to injective stores (since all variables and constants are mapped to distinct locations), which greatly simplifies the handling of equalities.

The main ingredient used to define core formulæ are *context predicates*. Given a tuple of predicate symbols $(p, q_1, \ldots, q_n) \in \mathbb{P}^{n+1}$, where $n \geq 0$, we consider a context predicate symbol $\Gamma_{p,q_1,\ldots,q_n}$ of arity $\#p + \sum_{i=1}^{n} \#q_i$. The informal intuition of a context predicate atom $\Gamma_{p,q_1,\ldots,q_n}(\mathbf{t}, \mathbf{u}_1, \ldots, \mathbf{u}_n)$ is the following: a structure $(\mathfrak{s}, \mathfrak{h})$ is a model of this atom if there exist models $(\mathfrak{s}, \mathfrak{h}_i)$ of $q_i(\mathbf{u}_i)$, $i \in [\![1 \,..\, n]\!]$ respectively, with mutually disjoint heaps, an unfolding ψ of $p(\mathbf{t})$ in which the atoms $q_i(\mathbf{u}_i)$ occur, and an associate $\mathfrak{s}'$ of $\mathfrak{s}$ such that $(\mathfrak{s}', \mathfrak{h} \uplus \biguplus_{i=1}^{n} \mathfrak{h}_i)$ is a model of ψ.

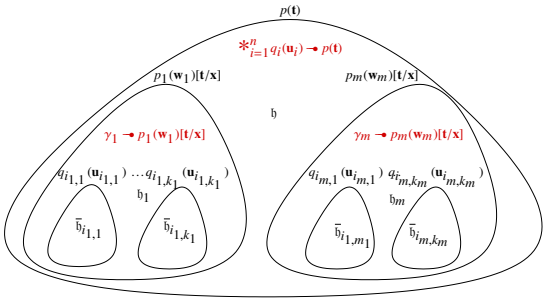

Figure 1 Inductive Definition of Context Predicates

For readability's sake, we adopt a notation close in spirit to SL's separating implication (known as the magic wand), and we write $*_{i=1}^{n} q_i(\mathbf{y}_i) \twoheadrightarrow p(\mathbf{x})$ for $\Gamma_{p,q_1,\ldots,q_n}(\mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_n)$ and $\mathsf{emp} \twoheadrightarrow p(\mathbf{x})$, when $n = 0$[5]. The set of rules defining the interpretation of context predicates is the least set defined by the inference rules below, denoted $\mathfrak{C}_{\mathcal{S}}$:

$$\frac{}{p(\mathbf{x}) \twoheadrightarrow p(\mathbf{y}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \mathbf{x} \doteq \mathbf{y}} \; \mathbf{x} \cap \mathbf{y} = \emptyset \qquad \text{(I)}$$

$$\frac{p(\mathbf{x}) \Leftarrow_{\mathcal{S}} \exists \mathbf{z} \,.\, \psi * *_{j=1}^{m} p_j(\mathbf{w}_j) \quad *_{i=1}^{n} q_i(\mathbf{y}_i) = *_{j=1}^{m} \gamma_j}{*_{i=1}^{n} q_i(\mathbf{y}_i) \twoheadrightarrow p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{v} \,.\, \psi\sigma * *_{j=1}^{m} \left(\gamma_j \twoheadrightarrow p_j(\sigma(\mathbf{w}_j))\right)} \; \begin{array}{l} \mathbf{x}, \mathbf{z}, \mathbf{y}_1, \ldots, \mathbf{y}_n \text{ pairwise disjoint} \\ \sigma : \mathbf{z} \rightharpoonup \mathbf{x} \cup \bigcup_{i=1}^{n} \mathbf{y}_i \\ \mathbf{v} = \mathbf{z} \setminus \mathrm{dom}(\sigma) \end{array} \qquad \text{(II)}$$

[5] Context predicates are similar to the *strong magic wand* introduced in [13]. A context predicate $\alpha \twoheadrightarrow \beta$ is also related to the usual separating implication $\alpha \mathrel{-\!\!*} \beta$ of separation logic, but it is not equivalent. Intuitively, $\mathrel{-\!\!*}$ represents a difference between two heaps, whereas $\twoheadrightarrow$ removes some atoms in an unfolding. For instance, if p and q are defined by the same inductive rules, up to a renaming of predicates, then $p(x) \mathrel{-\!\!*} q(x)$ always holds in a structure with an empty heap, whereas $p(x) \twoheadrightarrow q(x)$ holds if, moreover, $p(x)$ and $q(x)$ are the same atom.

Note that $\mathfrak{C}_\mathcal{S}$ is not progressing, since the rule for $p(\mathbf{x}) \multimap p(\mathbf{y})$ does not allocate any location. However, if $\mathcal{S}$ is progressing, then the set of rules obtained by applying (II) only is also progressing. Rule (I) says that each predicate atom $p(\mathbf{t}) \multimap p(\mathbf{u})$, such that $\mathbf{t}$ and $\mathbf{u}$ are mapped to the same tuple of locations, is satisfied by the empty heap. To understand rule (II), let $(\mathfrak{s}, \mathfrak{h})$ be an $\mathcal{S}$-model of $p(\mathbf{t})$ and assume there are a predicate-free unfolding ψ of $p(\mathbf{t})$ and an associate $\mathfrak{s}'$ of $\mathfrak{s}$, such that $q_1(\mathbf{u}_1), \ldots, q_n(\mathbf{u}_n)$ occur in ψ and $(\mathfrak{s}', \mathfrak{h}) \models_\mathcal{S} \psi$ (Fig. 1). If the first unfolding step is an instance of a rule $p(\mathbf{x}) \Leftarrow_\mathcal{S} \exists \mathbf{z} \,.\, \psi * \mathop{\ast}_{j=1}^{m} p_j(\mathbf{w}_j)$ then there exist a $\mathbf{z}$-associate $\overline{\mathfrak{s}}$ of $\mathfrak{s}$ and a split of $\mathfrak{h}$ into disjoint heaps $\mathfrak{h}_0, \ldots, \mathfrak{h}_m$ such that $(\overline{\mathfrak{s}}, \mathfrak{h}_0) \models \psi[\mathbf{t}/\mathbf{x}]$ and $(\overline{\mathfrak{s}}, \mathfrak{h}_j) \models_\mathcal{S} \mathop{\ast}_{j=1}^{m} p_j(\mathbf{w}_j)[\mathbf{t}/\mathbf{x}]$, for all $j \in [\![1 \,..\, m]\!]$. Assume, for simplicity, that $\mathbf{u}_1 \cup \ldots \cup \mathbf{u}_n \subseteq \mathrm{dom}(\overline{\mathfrak{s}})$ and let $\overline{\mathfrak{h}}_1, \ldots, \overline{\mathfrak{h}}_n$ be disjoint heaps such that $(\overline{\mathfrak{s}}, \overline{\mathfrak{h}}_i) \models_\mathcal{S} q_i(\mathbf{u}_i)$. Then there exists a partition $\{\{i_{j,1}, \ldots, i_{j,k_j}\} \mid j \in [\![1 \,..\, m]\!]\}$ of $[\![1 \,..\, n]\!]$, such that $\overline{\mathfrak{h}}_{i_{j,1}}, \ldots, \overline{\mathfrak{h}}_{i_{j,k_j}} \subseteq \mathfrak{h}_j$, for all $j \in [\![1 \,..\, m]\!]$. Let $\gamma_j \stackrel{\text{def}}{=} \mathop{\ast}_{\ell=1}^{k_j} q_\ell(\mathbf{u}_\ell)$, then $(\overline{\mathfrak{s}}, \mathfrak{h}_j \setminus (\overline{\mathfrak{h}}_{i_{j,1}} \cup \ldots \cup \overline{\mathfrak{h}}_{i_{j,k_j}})) \models_{\mathfrak{C}_\mathcal{S}} \gamma_j \multimap p_j(\mathbf{w}_j)[\mathbf{t}/\mathbf{x}]$, for each $j \in [\![1 \,..\, m]\!]$. This observation leads to the inductive definition of the semantics for $\mathop{\ast}_{i=1}^{n} q_i(\mathbf{u}_i) \multimap p(\mathbf{t})$, by the rule that occurs in the conclusion of (II), where the substitution $\sigma : \mathbf{z} \rightharpoonup \mathbf{x} \cup \bigcup_{i=1}^{n} \mathbf{y}_i$ is used to instantiate[6] some of the existentially quantified variables from the original rule $p(\mathbf{x}) \Leftarrow_\mathcal{S} \exists \mathbf{z} \,.\, \psi * \mathop{\ast}_{j=1}^{m} p_j(\mathbf{w}_j)$.

▶ **Example 18.** Consider the set $\mathcal{S} = \{p(x) \Leftarrow \exists z_1, z_2 \,.\, x \mapsto (z_1, z_2) * q(z_1) * q(z_2), q(x) \Leftarrow x \mapsto (x, x)\}$. We have $(\mathfrak{s}, \mathfrak{h}) \models_\mathcal{S} p(x)$ with $\mathfrak{s} = \{(x, \ell_1)\}$ and $\mathfrak{h} = \{(\ell_1, \ell_2, \ell_3), (\ell_2, \ell_2, \ell_2), (\ell_3, \ell_3, \ell_3)\}$. The atom $q(y) \multimap p(x)$ is defined by the following non-progressing rules:

$$q(y) \multimap p(x) \quad \Leftarrow \quad \exists z_1, z_2 \,.\, x \mapsto (z_1, z_2) * q(y) \multimap q(z_1) * \mathsf{emp} \multimap q(z_2) \qquad q(y) \multimap q(x) \quad \Leftarrow \quad x \doteq y$$
$$q(y) \multimap p(x) \quad \Leftarrow \quad \exists z_1, z_2 \,.\, x \mapsto (z_1, z_2) * \mathsf{emp} \multimap q(z_1) * q(y) \multimap q(z_2) \qquad \mathsf{emp} \multimap q(x) \quad \Leftarrow \quad x \mapsto (x, x)$$

The two rules for $q(y) \multimap p(x)$ correspond to the two ways of distributing $q(y)$ over $q(z_1)$, $q(z_2)$. We have $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$, with $\mathfrak{h}_1 = \{(\ell_1, \ell_2, \ell_3), (\ell_2, \ell_2, \ell_2)\}$ and $\mathfrak{h}_2 = \{(\ell_3, \ell_3, \ell_3)\}$. It is easy to check that $(\mathfrak{s}[y \leftarrow \ell_3], \mathfrak{h}_1) \models_{\mathfrak{C}_\mathcal{S}} q(y) \multimap p(x)$, and $(\mathfrak{s}[y \leftarrow \ell_3], \mathfrak{h}_2) \models_{\mathfrak{C}_\mathcal{S}} q(y)$. Note that we also have $(\mathfrak{s}[y \leftarrow \ell_2], \mathfrak{h}_1') \models_{\mathfrak{C}_\mathcal{S}} q(y) \multimap p(x)$, with $\mathfrak{h}_1' = \{(\ell_1, \ell_2, \ell_3), (\ell_3, \ell_3, \ell_3)\}$. ■

Having introduced context predicates, the pattern of core formulæ is defined below:

▶ **Definition 19.** *A* core formula φ *is an instance of the pattern:*

$$\exists_\mathsf{h} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \,.\, \mathop{\ast}_{i=1}^{n} \left(\mathop{\ast}_{j=1}^{k_i} q_j^i(\mathbf{u}_j^i) \multimap p_i(\mathbf{t}_i) \right) * \mathop{\ast}_{i=n+1}^{m} t_0^i \mapsto (t_1^i, \ldots, t_\aleph^i) \quad \textit{such that:}$$

(i) each variable occurring in $\mathbf{y}$ *also occurs in an atom in* φ*;*

(ii) for every variable $x \in \mathbf{x}$*, either* $x \in \mathbf{t}_i \setminus \bigcup_{i=1}^{k_i} \mathbf{u}_j^i$ *for some* $i \in [\![1 \,..\, n]\!]$*, or* $x = t_j^i$*, for some* $i \in [\![n+1 \,..\, m]\!]$ *and some* $j \in [\![0 \,..\, \aleph]\!]$*;*

(iii) each term t *occurs at most once as* $t = \mathsf{root}(\alpha)$*, where* α *is an atom of* φ*.*

We define moreover the set of terms $\mathrm{roots}(\varphi) \stackrel{\text{def}}{=} \mathrm{roots}_{\mathsf{lhs}}(\varphi) \cup \mathrm{roots}_{\mathsf{rhs}}(\varphi)$*, where* $\mathrm{roots}_{\mathsf{lhs}}(\varphi) \stackrel{\text{def}}{=} \{\mathsf{root}(q_j^i(\mathbf{u}_j^i)) \mid i \in [\![1 \,..\, n]\!], j \in [\![1 \,..\, k_i]\!]\}$ *and* $\mathrm{roots}_{\mathsf{rhs}}(\varphi) \stackrel{\text{def}}{=} \{\mathsf{root}(p_i(\mathbf{t}_i)) \mid i \in [\![1 \,..\, n]\!]\} \cup \{t_0^i \mid i \in [\![n+1 \,..\, m]\!]\}$.

Note that an unfolding of a core formula using the rules in $\mathfrak{C}_\mathcal{S}$ is not necessarily a core formula, because of the unbounded existential quantifiers and equational atoms that occur in the rules from $\mathfrak{C}_\mathcal{S}$. Note also that a core formula cannot contain an occurrence of a predicate of the form $p(\mathbf{t}) \multimap p(\mathbf{t})$ because otherwise, Condition (iii) of Definition 19 would be violated.

Lemma 20 shows that any symbolic heap is equivalent to an effectively computable finite disjunction of core formulæ, when the interpretation of formulæ is restricted to injective structures. For a

[6] Note that this instantiation is, in principle, redundant (i.e. the same rules are obtained if $\mathrm{dom}(\sigma) = \emptyset$ by chosing appropriate $\mathbf{z}$-associates) but we keep it to simplify the related proofs.

symbolic heap $\phi \in \mathsf{SH}^{\aleph}$, we define the set $\mathcal{T}(\phi)$, recursively on the structure of ϕ, implicitly assuming w.l.o.g. that $\mathsf{emp} * \phi = \phi * \mathsf{emp} = \phi$:

$$\mathcal{T}(\mathsf{emp}) \stackrel{\text{def}}{=} \{\mathsf{emp}\} \qquad \mathcal{T}(t_0 \mapsto (t_1,\ldots,t_{\aleph})) \stackrel{\text{def}}{=} \{t_0 \mapsto (t_1,\ldots,t_{\aleph})\}$$

$$\mathcal{T}(p(\mathbf{t})) \stackrel{\text{def}}{=} \{\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})\} \qquad \mathcal{T}\left(\mathbin{\raisebox{0.2ex}{$\scriptstyle\ast$}}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})\right) \stackrel{\text{def}}{=} \left\{\mathbin{\raisebox{0.2ex}{$\scriptstyle\ast$}}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})\right\}$$

$$\mathcal{T}(t_1 \doteq t_2) \stackrel{\text{def}}{=} \begin{cases} \{\mathsf{emp}\} & \text{if } t_1 = t_2 \\ \emptyset & \text{if } t_1 \neq t_2 \end{cases} \qquad \mathcal{T}(t_1 \neq t_2) \stackrel{\text{def}}{=} \begin{cases} \emptyset & \text{if } t_1 = t_2 \\ \{\mathsf{emp}\} & \text{if } t_1 \neq t_2 \end{cases}$$

$$\mathcal{T}(\phi_1 * \phi_2) \stackrel{\text{def}}{=} \{\psi_1 * \psi_2 \mid \psi_i \in \mathcal{T}(\phi_i),\ i = 1,2\}$$

$$\mathcal{T}(\exists x\,.\,\phi_1) \stackrel{\text{def}}{=} \{\exists_{\mathfrak{h}} x\,.\,\psi \mid \psi \in \mathcal{T}(\phi_1)\} \cup \{\psi \mid \psi \in \mathcal{T}(\phi_1[t/x]),\quad t \in (\mathsf{fv}(\phi_1) \setminus \{x\}) \cup \mathbb{C}\}$$

For instance, if $\phi = \exists x\,.\,p(x,y) * x \neq y$ and $\mathbb{C} = \{\mathsf{c}\}$, then $\mathcal{T}(\phi) = \{\exists_{\mathfrak{h}} x\,.\,\mathsf{emp} \mathrel{-\!\!\bullet} p(x,y),\ \mathsf{emp} \mathrel{-\!\!\bullet} p(\mathsf{c},y)\}$.

▶ **Lemma 20.** *Assume $\mathcal{S}$ is normalized. Consider an e-restricted normalized symbolic heap $\phi \in \mathsf{SH}^{\aleph}$ with no occurrences of context predicate symbols, and an injective structure $(\dot{\mathfrak{s}},\mathfrak{h})$, such that* $\mathrm{dom}(\dot{\mathfrak{s}}) = \mathsf{fv}(\phi) \cup \mathbb{C}$. *We have $(\dot{\mathfrak{s}},\mathfrak{h}) \models_{\mathcal{S}} \phi$ iff $(\dot{\mathfrak{s}},\mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \psi$, for some $\psi \in \mathcal{T}(\phi)$.*

Next, we give an equivalent condition for the satisfaction of a context predicate atom, that relies on an unfolding of a symbolic heap into a core formula:

▶ **Definition 21.** *A formula φ is a* core unfolding *of a predicate atom $\mathbin{\raisebox{0.2ex}{$\scriptstyle\ast$}}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$, written $\mathbin{\raisebox{0.2ex}{$\scriptstyle\ast$}}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} \varphi$, iff there exists:*

1. *a rule $\mathbin{\raisebox{0.2ex}{$\scriptstyle\ast$}}_{i=1}^{n} q_i(\mathbf{y}_i) \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{z}\,.\,\phi$, where ϕ is quantifier free, and*
2. *a substitution $\sigma = [\mathbf{t}/\mathbf{x}, \mathbf{u}_1/\mathbf{y}_1, \ldots, \mathbf{u}_n/\mathbf{y}_n] \cup \zeta$, $\zeta \subseteq \{(z,t) \mid z \in \mathbf{z},\ t \in \mathbf{t} \cup \bigcup_{i=1}^{n} \mathbf{u}_i\}$, such that $\varphi \in \mathcal{T}(\phi\sigma)$.*

A core unfolding of a predicate atom is always a quantifier-free formula, obtained from the translation (into a disjunctive set of core formulæ) of the quantifier-free matrix of the body of a rule, in which some of the existentially quantified variables in the rule occur instantiated by the substitution σ. For instance, the rule $\mathsf{emp} \mathrel{-\!\!\bullet} p(x) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists y\,.\,x \mapsto y$ induces the core unfoldings $\mathsf{emp} \mathrel{-\!\!\bullet} p(a) \rightsquigarrow_{\mathcal{S}} a \mapsto a$ and $\mathsf{emp} \mathrel{-\!\!\bullet} p(a) \rightsquigarrow_{\mathcal{S}} a \mapsto u$, via the substitutions $[a/x, a/y]$ and $[a/x, u/y]$, respectively.

We now define a equivalence relation, of finite index, on the set of injective structures. Intuitively, an equivalence class is defined by the set of core formulæ that are satisfied by all structures in the class (with some additional conditions). First, we introduce the overall set of core formulæ, over which these equivalence classes are defined:

▶ **Definition 22.** *Let $\mathcal{V}_{\mathcal{P}} \stackrel{\text{def}}{=} \mathcal{V}^1_{\mathcal{P}} \cup \mathcal{V}^2_{\mathcal{P}}$, such that $\mathcal{V}^1_{\mathcal{P}} \cap \mathcal{V}^2_{\mathcal{P}} = \emptyset$ and $\|\mathcal{V}^i_{\mathcal{P}}\| = \mathrm{width}(\mathcal{P})$, for $i = 1,2$ and denote by* $\mathsf{Core}(\mathcal{P})$ *the set of core formulæ φ such that* $\mathrm{roots}(\varphi) \cap \mathsf{fv}(\varphi) \subseteq \mathcal{V}^1_{\mathcal{P}}$, $\mathrm{roots}(\varphi) \setminus \mathsf{fv}(\varphi) \subseteq \mathcal{V}^2_{\mathcal{P}} \cup \mathbb{C}$ *and no variable in $\mathcal{V}^1_{\mathcal{P}}$ is bound in φ.*

Note that $\mathsf{Core}(\mathcal{P})$ is a finite set, because both $\mathcal{V}_{\mathcal{P}}$ and $\mathbb{C}$ are finite. Intuitively, $\mathcal{V}^1_{\mathcal{P}}$ will denote "local" variables introduced by unfolding the definitions on the left-hand sides of the entailments, whereas $\mathcal{V}^2_{\mathcal{P}}$ will denote existential variables occurring on the right-hand sides. Second, we characterize an injective structure by the set of core formulæ it satisfies:

▶ **Definition 23.** *For a core formula $\varphi = \exists_{\mathfrak{h}} \mathbf{x} \forall_{\neg \mathfrak{h}} \mathbf{y}\,.\,\psi$, we denote by $\mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}},\mathfrak{h},\varphi)$ the set of stores $\dot{\bar{\mathfrak{s}}}$ that are injective $(\mathbf{x} \cup \mathbf{y})$-associates of $\dot{\mathfrak{s}}$, and such that: (1) $(\dot{\bar{\mathfrak{s}}},\mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \psi$, (2) $\dot{\bar{\mathfrak{s}}}(\mathbf{x}) \subseteq \mathrm{loc}(\mathfrak{h})$, and (3) $\dot{\bar{\mathfrak{s}}}(\mathbf{y}) \cap \mathrm{loc}(\mathfrak{h}) = \emptyset$. The elements of this set are called* witnesses for $(\dot{\mathfrak{s}},\mathfrak{h})$ and φ.

The core abstraction *of an injective structure $(\dot{\mathfrak{s}},\mathfrak{h})$ is the set $C_{\mathcal{P}}(\dot{\mathfrak{s}},\mathfrak{h})$ of core formulæ $\varphi \in \mathsf{Core}(\mathcal{P})$ for which there exists a witness $\dot{\bar{\mathfrak{s}}} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}},\mathfrak{h},\varphi)$ such that $\dot{\bar{\mathfrak{s}}}(\mathrm{roots}_{\mathsf{lhs}}(\varphi)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$.*

An injective structure $(\dot{\mathfrak{s}},\mathfrak{h})$ satisfies each core formula $\varphi \in C_{\mathcal{P}}(\dot{\mathfrak{s}},\mathfrak{h})$[7], fact that is witnessed by an extension of the store assigning the universally quantified variables random locations outside of the heap. Further, any core formula φ such that $(\dot{\mathfrak{s}},\mathfrak{h}) \models \varphi$ and $\mathrm{roots}_{\mathsf{lhs}}(\varphi) = \emptyset$ occurs in $C_{\mathcal{P}}(\dot{\mathfrak{s}},\mathfrak{h})$.

[7] An easy consequence of Lemma 52 in Appendix H.

Our entailment checking algorithm relies on the definition of the *profile* of a symbolic heap. Since each symbolic heap is equivalent to a finite disjunction of existential core formulæ, when interpreted over injective normal structures, it is sufficient to consider only profiles of core formulæ:

▶ **Definition 24.** *A* profile *for an entailment problem* $\mathcal{P} = (\mathcal{S}, \Sigma)$ *is a relation* $\mathcal{F} \subseteq \mathsf{Core}(\mathcal{P}) \times 2^{\mathsf{Core}(\mathcal{P})}$ *such that, for any core formula* $\phi \in \mathsf{Core}(\mathcal{P})$ *and any set of core formulæ* $F \in 2^{\mathsf{Core}(\mathcal{P})}$*, we have* $(\phi, F) \in \mathcal{F}$ *iff* $F = C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h})$*, for some injective normal* $\mathfrak{C}_{\mathcal{S}}$*-model* $(\dot{\mathfrak{s}}, \mathfrak{h})$ *of* ϕ*, with* $\mathrm{dom}(\dot{\mathfrak{s}}) = \mathsf{fv}(\phi) \cup \mathbb{C}$.

Assuming the existence of a profile, the effective construction of which will be given in Section 6, the following lemma provides an algorithm that decides the validity of $\mathcal{P}$:

▶ **Lemma 25.** *Let* $\mathcal{P} = (\mathcal{S}, \Sigma)$ *be a normalized e-restricted entailment problem and* $\mathcal{F} \subseteq \mathsf{Core}(\mathcal{P}) \times 2^{\mathsf{Core}(\mathcal{P})}$ *be a profile for* $\mathcal{P}$*. Then* $\mathcal{P}$ *is valid iff, for each sequent* $\phi \vdash_{\mathcal{P}} \psi_1, \ldots, \psi_n$*, each core formula* $\varphi \in \mathcal{T}(\phi)$ *and each pair* $(\varphi, F) \in \mathcal{F}$*, we have* $F \cap \mathcal{T}(\psi_i) \neq \emptyset$*, for some* $i \in [\![1 \,..\, n]\!]$.

The proof relies on Lemma 17, according to which entailments can be tested by considering only normal models. As one expects, Lemma 20 is used in this proof to ensure that the translation $\mathcal{T}(.)$ of symbolic heaps into core formulæ preserves the injective models.

6 Construction of the Profile Function

For a given normalized entailment problem $\mathcal{P} = (\mathcal{S}, \Sigma)$, describe the construction of a profile $\mathcal{F}_{\mathcal{P}} \subseteq \mathsf{Core}(\mathcal{P}) \times 2^{\mathsf{Core}(\mathcal{P})}$, recursively on the structure of core formulæ. We assume that the set of rules $\mathcal{S}$ is progressing, connected and e-restricted. The relation $\mathcal{F}_{\mathcal{P}}$ is the least set satisfying the recursive constraints (1), (2), (3) and (4), given in this section. Since these recursive definitions are monotonic, the least fixed point exists and is unique. We shall prove later (Theorem 32) that the least fixed point can, moreover, be attained in a finite number of steps by a standard Kleene iteration.

Points-to Atoms For a points-to atom $t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}})$, such that $t_0, \ldots, t_{\mathfrak{K}} \in \mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C}$, we have:

$$(t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}}),\ F) \in \mathcal{F}_{\mathcal{P}}, \text{ iff } F \text{ is the set containing } t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}}) \text{ and all core formulæ of the form } \forall_{\neg \mathfrak{h}} \mathbf{z} \,.\, \circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \in \mathsf{Core}(\mathcal{P}), \text{ where } \mathbf{z} = (\mathbf{t} \cup \mathbf{u}_1 \cup \ldots \cup \mathbf{u}_n) \setminus (\{t_0, \ldots, t_{\mathfrak{K}}\} \cup \mathbb{C}) \text{ such that } \mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}}) * \circledast_{i=1}^{n} \mathsf{emp} \mathrel{-\!\!\bullet} q_i(\mathbf{u}_i) \quad (1)$$

For instance, if $\mathcal{S} = \{p(x) \Leftarrow \exists y, z \,.\, x \mapsto y * q(y,z),\ q(x,y) \Leftarrow x \mapsto y\}$, with $\mathcal{V}^1_{\mathcal{P}} = \{u, v\}$ and $\mathcal{V}^2_{\mathcal{P}} = \{z\}$, then $\mathcal{F}_{\mathcal{P}}$ contains the pair $(u \mapsto v, F)$ with $F = \{u \mapsto v, \mathsf{emp} \mathrel{-\!\!\bullet} q(u,v), \forall_{\neg \mathfrak{h}} z \,.\, q(v,z) \mathrel{-\!\!\bullet} p(u)\}$.

Predicate Atoms Since profiles involve only the core formulæ obtained by the syntactic translation of a symbolic heap, the only predicate atoms that occur in the argument of a profile are of the form $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$. We consider the constraint:

$$(\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}),\ F) \in \mathcal{F}_{\mathcal{P}} \text{ if } (\exists_{\mathfrak{h}} \mathbf{y} \,.\, \psi,\ F) \in \mathcal{F}_{\mathcal{P}}, \mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} \psi \in \mathsf{Core}(\mathcal{P}) \text{ and } \mathbf{y} = \mathsf{fv}(\psi) \setminus \mathbf{t} \quad (2)$$

Separating Conjunctions Computing the profile of a separating conjunction is the most technical point of the construction. To ease the presentation, we assume the existence of a binary operation called *composition*:

▶ **Definition 26.** *Given a set* $D \subseteq \mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C}$*, a binary operator* $\circledast_D : 2^{\mathsf{Core}(\mathcal{P})} \times 2^{\mathsf{Core}(\mathcal{P})} \to 2^{\mathsf{Core}(\mathcal{P})}$ *is a* composition *if* $C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}_1) \circledast_D C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}_2) = C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h})$*, for any injective structure* $(\dot{\mathfrak{s}}, \mathfrak{h})$*, such that (i)* $\mathrm{dom}(\dot{\mathfrak{s}}) \subseteq \mathcal{V}^1_{\mathcal{P}}$*, (ii)* $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$*, (iii)* $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \subseteq \dot{\mathfrak{s}}(\mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C})$*, (iv)* $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \cap \mathrm{dom}(\mathfrak{h}) \subseteq \dot{\mathfrak{s}}(D) \subseteq \mathrm{dom}(\mathfrak{h})$.

We recall that $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) = \mathrm{loc}(\mathfrak{h}_1) \cap \mathrm{loc}(\mathfrak{h}_2)$. If $\mathcal{S}$ is a normalized set of rules, then for any core formula ϕ whose only occurrences of predicate atoms are of the form $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$, we define $\mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi)$ as the homomorphic extension of $\mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})) \stackrel{\text{def}}{=} \mathsf{alloc}_{\mathcal{S}}(p(\mathbf{t}))$ to ϕ (see Definition 9). Assuming

that $\mathcal{S}$ is a normalized set of rules and that a composition operation $\circledast_D$ (the construction of which will be described below, see Lemma 30) exists, we define the profile of a separating conjunction:

$$(\phi_1 * \phi_2, \mathsf{add}(X_1, F_1) \circledast_D \mathsf{add}(X_2, F_2)) \in \mathcal{F}_{\mathcal{P}}, \text{ if } (\phi_i, F_i) \in \mathcal{F}_{\mathcal{P}} \;\; X_i \stackrel{\text{def}}{=} \mathsf{fv}(\phi_{3-i}) \setminus \mathsf{fv}(\phi_i), \; i = 1, 2$$
$$\mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_1) \cap \mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_2) = \emptyset, \;\; D \stackrel{\text{def}}{=} \mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_1 * \phi_2) \cap (\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C}) \tag{3}$$
$$\mathsf{add}(x, F) \stackrel{\text{def}}{=} \{\exists_{\mathsf{h}} \mathbf{y} \forall_{\neg \mathsf{h}} \mathbf{z} \,.\, \psi \mid \exists_{\mathsf{h}} \mathbf{y} \forall_{\neg \mathsf{h}} \mathbf{z} \forall_{\neg \mathsf{h}} \hat{x} \,.\, \psi[\hat{x}/x] \in F\}, \; \mathsf{add}(\{x_1, \ldots, x_n\}, F) \stackrel{\text{def}}{=} \mathsf{add}(x_1, \ldots \mathsf{add}(x_n, F))$$

The choice of the set D above ensures (together with the restriction to normal models) that $\circledast_D$ is indeed a composition operator. Intuitively, since the considered models are normal, every location in the frontier between the heaps corresponding to ϕ_1 and ϕ_2 will be associated with a variable, thus D denotes the set of allocated locations on the frontier. Note that, because $\mathcal{P}$ is normalized, $\mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_1 * \phi_2)$ is well-defined. Because the properties of the composition operation hold when the models of its operands share the same store (Definition 26), we use the $\mathsf{add}(x, F)$ function that adds free variables (mapped to locations outside of the heap) to each core formula in F.

Existential Quantifiers Since profiles involve only core formulæ obtained by the syntactic translation of a symbolic heap (Lemma 25), it is sufficient to consider only existentially quantified core formulæ, because the syntactic translation $\mathcal{T}(.)$ does not produce universal quantifiers. The profile of an existentially quantified core formula is given by the constraint:

$$(\exists_{\mathsf{h}} x' \,.\, \phi[x'/x], \; \mathsf{rem}(x, F)) \in \mathcal{F}_{\mathcal{P}}, \text{ if } x \in \mathsf{fv}(\phi), \; x' \in \mathcal{V}^2_{\mathcal{P}}, \; x' \text{ not bound in } \phi, \; (\phi, F) \in \mathcal{F}_{\mathcal{P}}, \tag{4}$$
$$\mathsf{rem}(x, F) \stackrel{\text{def}}{=} \{\exists_{\mathsf{h}} \hat{x} \,.\, \psi[\hat{x}/x] \mid \psi \in F, \; x \in \mathsf{fv}(\psi), \; \hat{x} \text{ not in } \psi\} \cap \mathsf{Core}(\mathcal{P}) \cup \{\psi \mid \psi \in F, \; x \notin \mathsf{fv}(\psi)\}$$
$$\mathsf{rem}(\{x_1, \ldots, x_n\}, F) \stackrel{\text{def}}{=} \mathsf{rem}(x_1, \ldots \mathsf{rem}(x_n, F) \ldots)$$

Note that $\hat{x}$ is a fresh variable, which is not bound or free in ψ. In particular, if $x \in \mathsf{roots}(\psi)$, then we must have $\hat{x} \in \mathcal{V}^2_{\mathcal{P}}$, so that $\exists_{\mathsf{h}} \hat{x} \,.\, \psi[\hat{x}/x] \in \mathsf{Core}(\mathcal{P})$. Similarly the variable x is replaced by a fresh variable $x' \in \mathcal{V}^2_{\mathcal{P}}$ in $\exists_{\mathsf{h}} x' \,.\, \phi[x'/x]$ to ensure that $\exists_{\mathsf{h}} x' \,.\, \phi[x'/x]$ is a core formula.

The Profile Function Let $\mathcal{F}_{\mathcal{P}}$ be the least relation that satisfies the constraints (1), (2), (3) and (4). We prove that $\mathcal{F}_{\mathcal{P}}$ is a valid profile for $\mathcal{P}$, in the sense of Definition 24:

▶ **Lemma 27.** *Given a progressing and normalized entailment problem $\mathcal{P} = (\mathcal{S}, \Sigma)$, a symbolic heap $\varphi \in \mathsf{SH}^{\Re}$ with $\mathsf{fv}(\varphi) \subseteq \mathcal{V}^1_{\mathcal{P}}$, a core formula $\phi \in \mathcal{T}(\varphi)$ and a set of core formulæ $F \subseteq \mathsf{Core}(\mathcal{P})$, we have $(\phi, F) \in \mathcal{F}_{\mathcal{P}}$ iff $F = C_{\mathcal{P}}(\mathfrak{s}, \mathfrak{h})$, for some injective normal $\mathfrak{C}_{\mathcal{S}}$-model $(\mathfrak{s}, \mathfrak{h})$ of ϕ, with $\mathrm{dom}(\mathfrak{s}) = \mathsf{fv}(\varphi) \cup \mathbb{C}$.*

The composition operation $\circledast_D$ works symbolically on core formulæ, by saturating the separating conjunction of two core formulæ via a *modus ponens*-style consequence operator.

▶ **Definition 28.** *Given formulæ ϕ, ψ, we write $\phi \Vdash \psi$ if $\phi = \varphi * [\alpha \multimap p(\mathbf{t})] * [(\beta * p(\mathbf{t})) \multimap q(\mathbf{u})]$ and $\psi = \varphi * [(\alpha * \beta) \multimap q(\mathbf{u})]$ (up to the commutativity of $*$ and the neutrality of emp) for some formula φ, predicate atoms $p(\mathbf{t})$ and $q(\mathbf{u})$ and conjunctions of predicate atoms α and β.*

▶ **Example 29.** Consider the structure $(\mathfrak{s}, \mathfrak{h})$ and the rules of Example 18. We have $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$, with $(\mathfrak{s}[y \leftarrow \ell_3], \mathfrak{h}_1) \models_{\mathfrak{C}_{\mathcal{S}}} q(y) \multimap p(x)$ and $(\mathfrak{s}[y \leftarrow \ell_3], \mathfrak{h}_2) \models_{\mathcal{S}} q(y)$, i.e., $(\mathfrak{s}[y \leftarrow \ell_3], \mathfrak{h}_2) \models_{\mathfrak{C}_{\mathcal{S}}} \mathsf{emp} \multimap q(y)$, thus $(\mathfrak{s}[y \leftarrow \ell_3], \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} q(y) \multimap p(x) * \mathsf{emp} \multimap q(y) \Vdash \mathsf{emp} \multimap p(x)$. ■

We define a relation on the set of core formulæ $\mathsf{Core}(\mathcal{P})$, parameterized by a set $D \subseteq \mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C}$:

$$\exists_{\mathsf{h}} \mathbf{x}_1 \forall_{\neg \mathsf{h}} \mathbf{y}_1 \,.\, \psi_1, \exists_{\mathsf{h}} \mathbf{x}_2 \forall_{\neg \mathsf{h}} \mathbf{y}_2 \,.\, \psi_2 \Vdash\!\!\!\Vdash_D \exists_{\mathsf{h}} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \,.\, \psi \tag{5}$$
$$\text{if } \psi_1 * \psi_2 \Vdash^* \psi, \mathbf{x}_1 \cap \mathbf{x}_2 = \emptyset, \mathbf{x} = (\mathbf{x}_1 \cup \mathbf{x}_2) \cap \mathsf{fv}(\psi), \mathbf{y} = ((\mathbf{y}_1 \cup \mathbf{y}_2) \cap \mathsf{fv}(\psi)) \setminus \mathbf{x}, \mathrm{roots}_{\mathsf{lhs}}(\psi) \cap D = \emptyset.$$

The composition operator is defined by lifting the $\Vdash\!\!\!\Vdash$ relation to sets of core formulæ:

$$F_1 \circledast_D F_2 \stackrel{\text{def}}{=} \{\psi \mid \phi_1 \in F_1, \phi_2 \in F_2, \phi_1, \phi_2 \Vdash\!\!\!\Vdash_D \psi\} \tag{6}$$

We show that $\circledast_D$ is indeed a composition, in the sense of Definition 26:

▶ **Lemma 30.** *Let $\mathcal{S}$ be a normalized, progressing, connected and e-restricted set of rules, $D \subseteq \mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C}$ be a set of terms and $(\dot{\mathfrak{s}}, \mathfrak{h})$ be an injective structure, with $\mathrm{dom}(\dot{\mathfrak{s}}) \subseteq \mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C}$. Let $\mathfrak{h}_1$ and $\mathfrak{h}_2$ be two disjoint heaps, such that: (1) $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$, (2) $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \subseteq \dot{\mathfrak{s}}(\mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C})$ and (3) $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \cap \mathrm{dom}(\mathfrak{h}) \subseteq \dot{\mathfrak{s}}(D) \subseteq \mathrm{dom}(\mathfrak{h})$. Then, we have $C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}) = C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}_1) \circledast_D C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}_2)$.*

7 Main Result

In this section, we state the main complexity result of the paper. As a prerequisite, we prove that the size of the core formulæ needed to solve an entailment problem $\mathcal{P}$ is polynomial in $\mathrm{width}(\mathcal{P})$ and the number of such formulæ is simply exponential in $\mathrm{width}(\mathcal{P}) + \log(\mathrm{size}(\mathcal{P}))$.

▶ **Lemma 31.** *Given an entailment problem $\mathcal{P}$, for every formula $\phi \in \mathsf{Core}(\mathcal{P})$, we have $\mathrm{size}(\phi) = O(\mathrm{width}(\mathcal{P})^2)$ and $\|\mathsf{Core}(\mathcal{P})\| = 2^{O(\mathrm{width}(\mathcal{P})^3 \times \log(\mathrm{size}(\mathcal{P})))}$.*

▶ **Theorem 32.** *Checking the validity of progressing, connected and e-restricted entailment problems is* 2-EXPTIME*-complete.*

Proof: 2-EXPTIME-hardness follows from [6]; since the reduction in [6] involves no (dis-)equality, the considered systems are trivially e-restricted. We now prove 2-EXPTIME-membership. Let $\mathcal{P}$ be an e-restricted problem. By Lemma 11, we compute, in time $\mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$, an equivalent normalized e-restricted problem $\mathcal{P}_n$ of $\mathrm{size}(\mathcal{P}_n) = \mathrm{size}(\mathcal{P}) \times 2^{O(\mathrm{width}(\mathcal{P})^2)}$ and $\mathrm{width}(\mathcal{P}_n) = O(\mathrm{width}(\mathcal{P})^2)$. We fix an arbitrary set of variables $\mathcal{V}_{\mathcal{P}_n} = \mathcal{V}^1_{\mathcal{P}_n} \uplus \mathcal{V}^2_{\mathcal{P}_n}$ with $\|\mathcal{V}^i_{\mathcal{P}_n}\| = \mathrm{width}(\mathcal{P}_n)$, for $i = 1, 2$ and we compute the relation $\mathcal{F}_{\mathcal{P}_n}$, using a Kleene iteration, as explained in Section 6 (Lemma 27). By Lemma 31, if $\psi \in \mathsf{Core}(\mathcal{P}_n)$ then $\mathrm{size}(\psi) = O(\mathrm{width}(\mathcal{P})^2)$ and if $(\psi, F) \in \mathcal{F}_{\mathcal{P}_n}$ then $\|F\| = 2^{O(\mathrm{width}(\mathcal{P}_n)^3 \times \log(\mathrm{size}(\mathcal{P}_n)))} = 2^{O(\mathrm{width}(\mathcal{P})^8 \times \log(\mathrm{size}(\mathcal{P})))}$, hence $\mathcal{F}_{\mathcal{P}}$ can be computed in $2^{2^{O(\mathrm{width}(\mathcal{P})^8 \times \log(\mathrm{size}(\mathcal{P})))}}$ steps. It thus suffices to check that each of these steps can be performed in polynomial time w.r.t. $\mathsf{Core}(\mathcal{P}_n)$ and $\mathrm{size}(\mathcal{P}_n)$. This is straightforward for points-to atoms, predicate atoms and existential formulæ, by iterating on the rules in $\mathcal{P}_n$ and applying the construction rules (1), (2) and (4) respectively. For the disjoint composition, one has to compute the relation $\Vdash^*$, needed to build the operator $\circledast_D$, according to (5) and (6). We use again a Kleene iteration. It is easy to check that $\phi \Vdash \psi \Rightarrow \mathrm{size}(\psi) \leq \mathrm{size}(\phi)$, furthermore, one only needs to check relations of the form $\phi_1 * \phi_2 \Vdash \psi$ with $\phi_1, \phi_2, \psi \in \mathsf{Core}(\mathcal{P}_n)$. This entails that the number of iteration steps is $2^{O(\mathrm{width}(\mathcal{P})^8 \times \log(\mathrm{size}(\mathcal{P})))}$ and, moreover, each step can be performed in time polynomial w.r.t. $\mathsf{Core}(\mathcal{P}_n)$. Finally, we apply Lemma 25 to check that all the entailments in $\mathcal{P}_n$ are valid. This test can be performed in time polynomial w.r.t. $\|\mathcal{F}_{\mathcal{P}_n}\|$ and $\mathrm{size}(\mathcal{P}_n)$. ◀

8 Conclusion and Future Work

We presented a class of SL formulæ built from a set of inductively defined predicates, used to describe pointer-linked recursive data structures, whose entailment problem is 2-EXPTIME-complete. This fragment, consisting of so-called e-restricted formulæ, is a strict generalization of previous work defining three sufficient conditions for the decidability of entailments between SL formulæ, namely progress, connectivity and establishment [8, 12, 14]. On one hand, every progressing, connected and established entailment problem can be translated into an e-restricted problem. On the other hand, the models of e-restricted formulæ form a strict superset of the models of established formulæ. The proof for the 2-EXPTIME upper bound for e-restricted entailments leverages from a novel technique used to prove the upper bound of established entailments [12, 14]. A natural question is whether the e-restrictedness condition can be dropped. We conjecture that this is not the case, and that entailment is undecidable for progressing, connected and non-e-restricted sets. Another issue is whether the generalization of symbolic heaps to use guarded negation, magic wand and septraction from [15] is possible for e-restricted entailment problems. The proof of these conjectures is on-going work.

References

1 Timos Antonopoulos, Nikos Gorogiannis, Christoph Haase, Max I. Kanovich, and Joël Ouaknine. Foundations for decision problems in separation logic with general inductive predicates. In Anca Muscholl, editor, *FOSSACS 2014, ETAPS 2014, Proceedings*, volume 8412 of *Lecture Notes in Computer Science*, pages 411–425, 2014.

2 Josh Berdine, Byron Cook, and Samin Ishtiaq. Slayer: Memory safety for systems-level code. In Ganesh Gopalakrishnan andShaz Qadeer, editor, *Computer Aided Verification - 23rd International Conference, CAV 2011, Snowbird, UT, USA, July 14-20, 2011. Proceedings*, volume 6806 of *LNCS*, pages 178–183. Springer, 2011.

3 Cristiano Calcagno, Dino Distefano, Jérémy Dubreil, Dominik Gabi, Pieter Hooimeijer, Martino Luca, Peter W. O'Hearn, Irene Papakonstantinou, Jim Purbrick, and Dulma Rodriguez. Moving fast with software verification. In Klaus Havelund, Gerard J. Holzmann, and Rajeev Joshi, editors, *NASA Formal Methods - 7th International Symposium, NFM 2015, Pasadena, CA, USA, April 27-29, 2015, Proceedings*, volume 9058 of *LNCS*, pages 3–11. Springer, 2015.

4 Bruno Courcelle. The monadic second-order logic of graphs. i. recognizable sets of finite graphs. *Information and Computation*, 85(1):12 – 75, 1990.

5 Kamil Dudka, Petr Peringer, and Tomás Vojnar. Predator: A practical tool for checking manipulation of dynamic data structures using separation logic. In Ganesh Gopalakrishnan and Shaz Qadeer, editors, *Computer Aided Verification - 23rd International Conference, CAV 2011, Snowbird, UT, USA, July 14-20, 2011. Proceedings*, volume 6806 of *LNCS*, pages 372–378. Springer, 2011.

6 Mnacho Echenim, Radu Iosif, and Nicolas Peltier. Entailment checking in separation logic with inductive definitions is 2-exptime hard. In Elvira Albert and Laura Kovács, editors, *LPAR 2020: 23rd International Conference on Logic for Programming, Artificial Intelligence and Reasoning, Alicante, Spain, May 22-27, 2020*, volume 73 of *EPiC Series in Computing*, pages 191–211. EasyChair, 2020. URL: `https://easychair.org/publications/paper/DdNg`.

7 J. Flum and M. Grohe. *Parameterized Complexity Theory*. Springer-Verlag New York, Inc., 2006.

8 Radu Iosif, Adam Rogalewicz, and Jiri Simacek. The tree width of separation logic with recursive definitions. In *Proc. of CADE-24*, volume 7898 of *LNCS*, 2013.

9 Radu Iosif, Adam Rogalewicz, and Tomás Vojnar. Deciding entailments in inductive separation logic with tree automata. In Franck Cassez and Jean-François Raskin, editors, *ATVA 2014, Proceedings*, volume 8837 of *Lecture Notes in Computer Science*, pages 201–218. Springer, 2014.

10 Samin S Ishtiaq and Peter W O'Hearn. Bi as an assertion language for mutable data structures. In *ACM SIGPLAN Notices*, volume 36, pages 14–26, 2001.

11 Christina Jansen, Jens Katelaan, Christoph Matheja, Thomas Noll, and Florian Zuleger. Unified reasoning about robustness properties of symbolic-heap separation logic. In Hongseok Yang, editor, *Programming Languages and Systems (ESOP'17)*, pages 611–638. Springer Berlin Heidelberg, 2017.

12 Jens Katelaan, Christoph Matheja, and Florian Zuleger. Effective entailment checking for separation logic with inductive definitions. In Tomás Vojnar and Lijun Zhang, editors, *TACAS 2019, Proceedings, Part II*, volume 11428 of *Lecture Notes in Computer Science*, pages 319–336. Springer, 2019.

13 Koji Nakazawa, Makoto Tatsuta, Daisuke Kimura, and Mitsuru Yamamura. Cyclic Theorem Prover for Separation Logic by Magic Wand. In *ADSL 18 (First Workshop on Automated Deduction for Separation Logics)*, July 2018. Oxford, United Kingdom.

14 Jens Pagel, Christoph Matheja, and Florian Zuleger. Complete entailment checking for separation logic with inductive definitions, 2020. `arXiv:2002.01202`.

15 Jens Pagel and Florian Zuleger. Beyond symbolic heaps: Deciding separation logic with inductive definitions. In *LPAR-23*, volume 73 of *EPiC Series in Computing*, pages 390–408. EasyChair, 2020. URL: `https://easychair.org/publications/paper/VTGk`.

16 J.C. Reynolds. Separation Logic: A Logic for Shared Mutable Data Structures. In *Proc. of LICS'02*, 2002.

17 Neil Robertson and P.D Seymour. Graph minors. III. Planar tree-width. *Journal of Combinatorial Theory, Series B*, 36(1):49 – 64, 1984.

A Proof of Lemma 11 (Section 3)

Let $\mathcal{P} = (\mathcal{S}, \Sigma)$ be an input entailment problem. We transform $\mathcal{P}$ in order to meet points (1a), (1c), (2a), (2b) and (2c) of Definition 8, as follows.

(1a) First, we apply exhaustively, to each symbolic heap occurring in $\mathcal{P}$, the following transformations, for each term $t \in \mathbb{T}$:

$$\exists x \,.\, x \doteq t * \phi \quad \rightsquigarrow \quad \phi[t/x] \tag{7}$$

$$t \doteq t * \phi \quad \rightsquigarrow \quad \phi \tag{8}$$

Note that, at this point, there are no equality atoms involving an existentially quantified variable (recall that equalities between constants can be dismissed since they are either trivially false or equivalent to emp). We apply the following transformations, that introduce disequalities between the remaining existential variables and the rest of the terms.

$$p(\mathbf{x}) \Leftarrow \exists x \,.\, \rho \rightsquigarrow \left\{ \begin{array}{lll} p(\mathbf{x}) & \Leftarrow & \rho[t/x] \\ p(\mathbf{x}) & \Leftarrow & \exists x \,.\, \rho * x \neq t \end{array} \right\} \tag{9}$$

for all $t \in (\mathsf{fv}(\rho) \setminus \{x\}) \cup \mathbb{C}$, where $x \neq t$ does not occur in ρ

$$\phi \vdash \psi_1, \ldots, \exists x \,.\, \psi_i, \ldots, \psi_n \quad \rightsquigarrow \quad \phi \vdash \psi_1, \ldots, \psi_{i-1}, \psi_i[t/x], \exists x \,.\, x \neq t * \psi_i, \ldots, \psi_n \tag{10}$$

for all $t \in \mathbb{C}$, such that $x \neq t$ does not occur in ψ_i

Let $\mathcal{P}_1 = (\mathcal{S}_1, \Sigma_1)$ be the result of applying the transformations (7-10) exhaustively. Because every transformation preserves the equivalence of rules and sequents, $\mathcal{P}_1$ is valid iff $\mathcal{P}$ is valid. Note that, by Definition 3, there are no free variables occurring in a sequent from Σ. Then the only remaining equality atoms $t \doteq u$ occurring in $\mathcal{P}_1$ must occur in a rule $p(x_1, \ldots, x_{\#p}) \Leftarrow_{\mathcal{S}_1} \rho$ and neither t nor u can be an existentially quantified variable, hence $t, u \in \{x_1, \ldots, x_{\#p}\} \cup \mathbb{C}$. Before proceeding further with Condition (1a), we make sure that Condition (1c) is satisfied.

(1c) Let $q(t_1, \ldots, t_{\#q})$ be a predicate atom occurring in a rule or a sequent from $\mathcal{P}_1$, where $t_1, \ldots, t_{\#q} \in \mathbb{T}$, and let $(t_{i_1}, \ldots, t_{i_m})$ be the subsequence obtained by removing the terms from the set $\{t_i \mid i \in [\![1 \,..\, \#q]\!],\ \exists j < i \,.\, t_i = t_j\} \cup \mathbb{C}$ from $(t_1, \ldots, t_{\#q})$. We consider a fresh predicate symbol $q_{i_1,\ldots,i_m}$, of arity m, with the new rules $q_{i_1,\ldots,i_m}(x_1, \ldots, x_m) \Leftarrow \rho\sigma$, for each rule $q(x_1, \ldots, x_{\#q}) \Leftarrow_{\mathcal{S}} \rho$, where the substitution σ is defined such that, for all $j \in [\![1 \,..\, \#q]\!]$:

- $\sigma(x_j) \stackrel{\text{def}}{=} x_{i_\ell}$ if $t_j = t_{i_\ell}$, for some $\ell \in [\![1 \,..\, m]\!]$,
- $\sigma(x_j) \stackrel{\text{def}}{=} t_j$ if $t_j \in \mathbb{C}$, and
- $\sigma(x_j) \stackrel{\text{def}}{=} x_j$, otherwise.

Note that the definition of the sequence $(t_{i_1}, \ldots, t_{i_m})$ guarantees that such a substitution exists and it is unique. If the rule body obtained by applying the substitution σ contains a disequality $t \neq t$, for some $t \in \mathbb{T}$, we eliminate the rule. Otherwise, we apply transformation (8) to the newly obtained rule to eliminate trivial equalities. Finally, we replace each occurrence of $q(t_1, \ldots, t_{\#q})$ in $\mathcal{P}_1$ with $q_{i_1,\ldots,i_m}(t_{i_1}, \ldots, t_{i_m})$. Because $q(t_1, \ldots, t_m)$ and $q_{i_1,\ldots,i_m}(t_{i_1}, \ldots, t_{i_m})$ have the same step unfoldings, they have the same predicate-free unfoldings and this transformation preserves equivalence, yielding a problem that satisfies condition (1c). Let $\mathcal{P}_2 = (\mathcal{S}_2, \Sigma_2)$ be the outcome of this transformation, where $\mathcal{S}_2$ is the set of newly introduced rules and Σ_2 is obtained from Σ_1 by the replacement of each predicate atom $q(t_1, \ldots, t_{\#q})$ with $q_{i_1,\ldots,i_m}(t_{i_1}, \ldots, t_{i_m})$. It is easy to check that $\mathcal{P}_2$ and $\mathcal{P}_1$ have the same validity status, which is that of $\mathcal{P}$.

(1a) We will now finish the proof of Condition (1a). Since the transformation (7) removes equalities involving an existentially quantified variable and the equalities between constants can be eliminated as explained above, the only equalities that occur in the body of a rule $p(x_1, \ldots, x_{\#p}) \Leftarrow_{\mathcal{S}_2} \rho$ are of the form $x_i \doteq t$, where $i \in [\![1 \,..\, \#p]\!]$ and $t \in \{x_j \mid j \in [\![1 \,..\, \#p]\!], j \neq i\} \cup \mathbb{C}$. We show that if such an equality

occurs in the body of a rule, then this rule can safely be removed because any unfolding involving it generates an unsatisfiable symbolic heap. Let $p(u_1, \ldots, u_{\#p})$ be a predicate atom that occurs in a some unfolding of a symbolic heap from $\mathcal{P}$ and assume a step-unfolding that substitutes $p(u_1, \ldots, u_{\#p})$ with $\rho[u_1/x_1, \ldots, u_{\#p}/x_{\#p}]$. We distinguish two cases:

(i) $t = x_j$, for some $j \in [\![1 \,..\, \#p]\!] \setminus \{i\}$: by point (1c), u_i and u_j must be distinct terms. If $u_i, u_j \in \mathbb{C}$, then $u_i \neq u_j$ necessarily holds, by Assumption 1, thus the equality $x_i \doteq t$ is false when x_i, x_j are instantiated by u_i, u_j. Otherwise, if $u_i \in \mathbb{V}$ (the case $u_j \in \mathbb{V}$ is symmetric) then u_i and u_j were necessarily introduced by existential quantifiers, in which case the disequality $u_i \neq u_j$ has been asserted by transformations (9) or (10), thus $x_i \doteq t$ is false when x_i is replaced by u_i.

(ii) $t \in \mathbb{C}$: by a similar argument we show that that all the relevant instances of the equality $x_i \doteq t$ are unsatisfiable.

Consequently, if an equality occurs in a rule, then this the rule can safely be removed.

(1b) To ensure that all variables occur within a points-to or predicate atom, we apply exhaustively the following transformation to each symbolic heap in the problem:

$$\exists x \,.\, \ast_{i=1}^{n} x \neq t_i * \psi \rightsquigarrow \psi, \text{ if } x \notin \mathsf{fv}(\psi) \tag{11}$$

Let $\mathcal{P}_3 = (\mathcal{S}_3, \Sigma_2)$ be the outcome of this transformation. Because $\mathbb{L}$ is infinite, any formula $\exists x \,.\, \ast_{i=1}^{n} x \neq t_i$ is equivalent to emp. Consequently, $\mathcal{P}_3$ and $\mathcal{P}_2$ have the same validity status as $\mathcal{P}$ and $\mathcal{P}_3$ satisfies conditions (1a), (1b) and (1c).

(2a+2b) For each predicate symbol p that occurs in $\mathcal{S}_3$, we consider the predicate symbols $p_{X,Y,Z,A,B,C}$, of arities $\#p$ each, where (X, Y, Z) is a partition of $[\![1 \,..\, \#p]\!]$ and (A, B, C) is a partition of $\mathbb{C}$, along with the following rules: $p_{X,Y,Z,A,B,C}(x_1, \ldots, x_{\#p}) \Leftarrow \rho'$ if and only if $p(x_1, \ldots, x_{\#p}) \Leftarrow_{\mathcal{S}_3} \rho$ and ρ' is obtained from ρ by replacing each predicate atom $q(t_1, \ldots, t_{\#q})$ by a predicate atom $q_{X',Y',Z',A',B',C'}(t_1, \ldots, t_{\#q})$, for some partition (X', Y', Z') of $[\![1 \,..\, \#q]\!]$ and some partition (A', B', C') of $\mathbb{C}$, such that the following holds. For each $i \in [\![1 \,..\, \#p]\!]$:

- $i \in X$ iff either a points-to atom $x_i \mapsto (t_1, \ldots, t_{\mathfrak{K}})$ occurs in ρ, or ρ contains a predicate atom $r_{X'',Y'',Z'',A'',B'',C''}(t_1, \ldots, t_{\#r})$ such that $x_i = t_j$ and $j \in X''$,
- $i \in Y$ iff either $x_i \in \{t_1, \ldots, t_{\mathfrak{K}}\}$ for a points-to atom $t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}})$ occurring in ρ, or ρ contains a predicate atom $r_{X'',Y'',Z'',A'',B'',C''}(t_1, \ldots, t_{\#r})$ such that $x_i = t_j$ and $j \in Y''$.

Further, for each constant $c \in C$:

- $c \in A$ iff a points-to atom $c \mapsto (t_1, \ldots, t_{\mathfrak{K}})$ occurs in ρ or ρ contains a predicate atom $r_{X'',Y'',Z'',A'',B'',C''}(t_1, \ldots, t_{\#r})$ such that $c \in A''$,
- $c \in B$ iff either $c \in \{t_1, \ldots, t_{\mathfrak{K}}\}$, for a points-to atom $t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}})$ occurring in ρ or ρ contains a predicate atom $r_{X'',Y'',Z'',A'',B'',C''}(t_1, \ldots, t_{\#r})$ such that $c \in B''$,

Let Σ_4 (resp. $\mathcal{S}_4$) be the set of sequents (resp. rules) obtained by replacing each predicate atom $p(t_1, \ldots, t_{\#p})$ with $p_{X,Y,Z,A,B,C}(t_1, \ldots, t_{\#p})$, for some partition (X, Y, Z) of $[\![1 \,..\, \#p]\!]$ and some partition (A, B, C) of C. For each predicate symbol $p_{X,Y,Z,A,B,C}$ we consider a fresh predicate symbol $\overline{p}_{X,Y,A,B}$, of arity $\#\overline{p} \stackrel{\text{def}}{=} \#p - \|Z\|$, and each predicate atom $p_{X,Y,Z,A,B,C}(t_1, \ldots, t_{\#p})$ occurring in either $\mathcal{S}_4$ or Σ_4 is replaced by $\overline{p}_{X,Y,A,B}(t_{i_1}, \ldots, t_{i_m})$, where $t_{i_1}, \ldots, t_{i_m}$ is the subsequence of $t_1, \ldots, t_{\#p}$ obtained by removing the terms from $\{t_i \mid i \in Z\}$ and each atom involving these terms is removed from $\mathcal{S}_4$ and Σ_4. Let the result of this transformation be denoted by $\mathcal{P}_n = (\mathcal{S}_n, \Sigma_n)$, with $\mathsf{palloc}_{\mathcal{S}_n}(\overline{p}_{X,Y,A,B}) \stackrel{\text{def}}{=} X$ and $\mathsf{calloc}_{\mathcal{S}_n}(\overline{p}_{X,Y,A,B}) \stackrel{\text{def}}{=} A$. Properties 2a and 2b follow from the definition of the rules of $\overline{p}_{X,Y,A,B}$ by an easy induction on the length of the unfolding. The equivalence between the validity of $\mathcal{P}_n$ and the validity of $\mathcal{P}_4$ is based on the following:

▶ **Fact 1.** *Let ϕ be a symbolic heap occurring in a sequent from Σ_4, $\phi \Rightarrow^{*}_{\mathcal{S}_4} \psi$ be a predicate-free unfolding of ϕ and $p_{X,Y,Z,A,B,C}(t_1, \ldots, t_{\#p})$ be a predicate atom that occurs at some intermediate step of this predicate-free unfolding. Then each variable $t_i \in \mathsf{fv}(\psi)$, such that $i \in Z$, occurs existentially quantified in a subformula $\exists t_i \,.\, \ast_{j=1}^{n} t_i \neq u$ of ψ and nowhere else.*

Proof: Since $\mathsf{fv}(\phi) = \emptyset$, it must be the case that x_i has been introduced as an existentially quantified variable by an intermediate unfolding step. We show, by induction on the length of the unfolding from the point where the variable was introduced that t_i cannot occur in a points-to atom. ◀

Since $\mathbb{L}$ is infinite, any formula $\exists x \,.\, \circledast_{j=1}^{n} x \neq u_j$ is trivially satisfied in any structure $(\mathfrak{s}, \mathfrak{h})$, such that $\{u_1, \ldots, u_n\} \in \mathrm{dom}(\mathfrak{s})$. By Fact 1, it follows that eliminating the terms $\{t_i \mid i \in Z\}$ from each predicate atom $p_{X,Y,Z,A,B,C}(t_1, \ldots, t_{\#p})$ preserves equivalence.

(2c) The exhaustive application of rules (9) and (10), that add all possibe disequalities between existentially quantified variables and constants, ensures that Condition (2c) is satisfied. Consequently, $\mathcal{P}_n$ is normalized.

Assume now that $\mathcal{P}$ is e-restricted, namely that each equational atom $t \bowtie u$ occurring in $\mathcal{P}$ is such that $\{t, u\} \cap \mathbb{C} \neq \emptyset$. Note that the transformations (9) and (10) may introduce disequalities $x \neq t'$, where x is an existentially quantified variable. In the case where $\mathcal{P}$ is e-restricted, we apply these rules only for $t \in \mathbb{C}$. Suppose that, after applying rules (7-8) exhaustively, there exist some equality $t \simeq u$ in a rule, such that neither t nor u is an existentially quantified variable. But since $\mathcal{P}$ is e-restricted, $\{t, u\} \cap \mathbb{C} \neq \emptyset$ and this rule will be eliminated by the disequalities introduced by the modified versions of the transformations (9) and (10). Finally, if $\mathcal{P}$ is (strongly) established then $\mathcal{P}_n$ is (strongly) established, because the transformation does not introduce new existential quantifiers and preserves equivalence.

Let us now compute the time complexity of the normalization procedure and the width of the output entailment problem. Observe that transformations (7–10) either instantiate existentially quantified variables, add or remove equalities, thus they can be applied $O(\mathrm{size}(\mathcal{P}))$ times, increasing the width of the problem by at most $O(\mathrm{size}(\mathcal{P}))$. After the exhaustive application of transformations (7-10), the number of rules in $\mathcal{S}$ and the number of sequents in Σ has increased by a factor of $2^{\mathrm{width}(\mathcal{P})}$ and the width of the problem by a linear factor. Then $\mathrm{size}(\mathcal{P}_1) = O(\mathrm{size}(\mathcal{P}) \cdot 2^{\mathrm{width}(\mathcal{P})})$ and $\mathrm{width}(\mathcal{P}_1) = O(\mathrm{width}(\mathcal{P}))$. The transformation of step (1c) increases the number of rules in $\mathcal{S}_1$ by a factor of $2^{\alpha} = 2^{O(\mathrm{width}(\mathcal{P}_1))} = 2^{O(\mathrm{width}(\mathcal{P})^2)}$, where $\alpha = \max\{\#p \mid p(x_1, \ldots, x_{\#p}) \Leftarrow_{\mathcal{S}_1} \rho\} \leq \mathrm{width}(\mathcal{P})$ and does not change the width of the problem, i.e. $\mathrm{size}(\mathcal{P}_2) = \mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$ and $\mathrm{width}(\mathcal{P}_2) = O(\mathrm{width}(\mathcal{P})^2)$. Next, going from $\mathcal{P}_2$ to $\mathcal{P}_3$ does not increase the bounds on the size or width of the problem and we trivially obtain $\mathrm{size}(\mathcal{P}_3) = \mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$ and $\mathrm{width}(\mathcal{P}_3) = O(\mathrm{width}(\mathcal{P})^2)$. Finally, going from $\mathcal{P}_3$ to $\mathcal{P}_4$ increases the size of the problem by a factor of $2^{3\alpha} \cdot 2^{3\|\mathbb{C}\|}$ and, because $\|\mathbb{C}\| \leq \mathrm{width}(\mathcal{P})$, by the definition of $\mathrm{width}(\mathcal{P})$, we obtain $\mathrm{size}(\mathcal{P}_n) = \mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$ and $\mathrm{width}(\mathcal{P}_n) = O(\mathrm{width}(\mathcal{P})^2)$. Finally, the entire procedure has to be repeated for each partition $\mathfrak{C}$ of the set of constants $\mathbb{C}$. Since the number of partitions is $2^{O(\|\mathbb{C}\| \cdot \log_2 \|\mathbb{C}\|)} = 2^{O(\mathrm{width}(\mathcal{P}) \cdot \log_2 \mathrm{width}(\mathcal{P}))}$, we obtain that the size of the result is $\mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$. Since the increase in the size of the output problem is mirrored by the time required to obtain it, the execution of the procedure takes time $\mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$. ◀

B Proof of Theorem 13 (Section 3)

▶ **Lemma 33.** *Every established entailment problem* $\mathcal{P} = (\mathcal{S}, \Sigma)$ *can be reduced in time* $\mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$ *to a normalized and strongly established entailment problem* $\mathcal{P}_e$*, such that* $\mathrm{width}(\mathcal{P}_e) = O(\mathrm{width}(\mathcal{P})^2)$.

Proof: First, we use Lemma 11 to reduce $\mathcal{P}$ to an established normalized problem $\mathcal{P}_n = (\mathcal{S}_n, \Sigma_n)$ in time $\mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$, such that $\mathrm{size}(\mathcal{P}_n) = \mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$ and $\mathrm{width}(\mathcal{P}_n) = O(\mathrm{width}(\mathcal{P})^2)$. Second, given a symbolic heap ϕ and a variable x, we define the set of symbolic heaps $\mathcal{A}(\phi, x)$

recursively on the structure of ϕ, as follows:

$$\begin{array}{rcl} \mathcal{A}(t_1 \bowtie t_2, x) & \stackrel{\text{def}}{=} & \emptyset \\ \mathcal{A}(t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}}), x) & \stackrel{\text{def}}{=} & \{t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}}) * x \doteq t_0\} \\ \mathcal{A}(p(t_1, \ldots, t_{\#p}), x) & \stackrel{\text{def}}{=} & \left\{\overline{p}(x, t_1, \ldots, t_{\#p})\right\} \\ \mathcal{A}(\phi_1 * \phi_2, x) & \stackrel{\text{def}}{=} & \bigcup_{i=1,2} \{\phi_i * \psi \mid \psi \in \mathcal{A}(\phi_{3-i}, x)\} \end{array}$$

where $\overline{p}$ is a fresh predicate symbol not occurring in $\mathcal{P}$, of arity $\#\overline{p} \stackrel{\text{def}}{=} \#p + 1$ and the set of inductive rules is updated by replacing each rule $p(x_1, \ldots, x_{\#p}) \Leftarrow_{\mathcal{S}} \rho$ by the set of rules $\{\overline{p}(x_0, x_1, \ldots, x_{\#p}) \Leftarrow \psi \mid \psi \in \mathcal{A}(\rho, x_0)\}$. It is straightforward to show by induction that if $(\mathfrak{s}, \mathfrak{h})$ is a structure such that $(\mathfrak{s}, \mathfrak{h}) \models_{\mathcal{S}} \psi$ for some $\psi \in \mathcal{A}(\phi, x)$, then we have $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h})$. Observe that $\|\mathcal{A}(\phi, x)\| \leq 2^{\mathrm{size}(\phi)}$ and $\mathrm{size}(\psi) = O(\mathrm{size}(\phi))$, for each $\psi \in \mathcal{A}(\phi, x)$.

Let $\phi_0 \vdash_{\mathcal{P}_n} \phi_1, \ldots, \phi_n$ be a sequent from $\mathcal{P}_n$ and $(\mathfrak{s}, \mathfrak{h})$ be a structure such that $(\mathfrak{s}, \mathfrak{h}) \models_{\mathcal{S}_n} \phi_0$. By Definition 3, ϕ_0 is quantifier-free. Assume that $\phi_1 = \exists x \,.\, \psi_1$ (the argument is repeated for all existential quantifiers occurring in $\phi_1, \ldots, \phi_n$). Note that, since $\mathcal{P}_n$ is normalized, x occurs in a points-to or a predicate atom in ϕ_1. This implies that x necessarily occurs in a points-to atom in each symbolic heap φ_1 obtained by a predicate-free unfolding $\phi_1 \Rightarrow^*_{\mathcal{S}_n} \varphi_1$, by point (2a) of Definition 8. Thus, $\mathfrak{s}'(x) \in \mathrm{loc}(\mathfrak{h})$, for each x-associate $\mathfrak{s}'$ of $\mathfrak{s}$ such that $(\mathfrak{s}', \mathfrak{h}) \models \psi_1$. Since $\mathcal{S}_n$ is established, each location from $\mathrm{loc}(\mathfrak{h})$ belongs to $\mathfrak{s}(\mathbb{C}) \cup \mathrm{dom}(\mathfrak{h})$, thus $\mathfrak{s}'(x) \in \mathfrak{s}(\mathbb{C}) \cup \mathrm{dom}(\mathfrak{h})$. Hence ϕ_1 can safely be replaced by the set of symbolic heaps $\{\psi_1[t/x] \mid t \in \mathbb{C}\} \cup \{\exists x \,.\, \varphi \mid \varphi \in \mathcal{A}(\psi_1, x)\}$. Applying this transformation to each existentially quantified variable occurring in a sequent from $\mathcal{P}_n$ yields a strongly established problem $\mathcal{P}'$. Moreover, the reduction of $\mathcal{P}_n$ to $\mathcal{P}'$ requires $\mathrm{size}(\mathcal{P}_n) \cdot 2^{O(\mathrm{width}(\mathcal{P}_n))} = \mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$ time and the width of the outcome is $\mathrm{width}(\mathcal{P}') = O(\mathrm{width}(\mathcal{P}_n)) = O(\mathrm{width}(\mathcal{P})^2)$. ◀

C Proof of Theorem 13 (Section 3)

Lemma 33, we can reduce $\mathcal{P}$ to a normalized strongly established entailment problem $\mathcal{P}_e = (\mathcal{S}_e, \Sigma_e)$ in time $\mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$, such that $\mathrm{width}(\mathcal{P}_e) = O(\mathrm{width}(\mathcal{P})^2)$. Let $\phi \Rightarrow^*_{\mathcal{S}_e} \varphi$ be an arbitrary predicate-free unfolding of a symbolic heap ϕ on the right-hand side of a sequent in Σ_e, where $\varphi = \exists x_1 \ldots \exists x_n \,.\, \psi$ and ψ is quantifier-free. Because $\mathcal{P}_e$ is normalized, there are no equalities in ψ. Let $x \neq y$ be a disequality from ψ, where $\{x, y\} \cap \mathbb{C} = \emptyset$. By Definition 3, all variables from $\mathcal{P}_e$ are existentially quantified, thus it must be the case that $x, y \in \{x_1, \ldots, x_n\}$. Because $\mathcal{P}_e$ is strongly established, ϕ is $\mathcal{S}_e$-established, thus both x and y are allocated in ψ. Moreover, since there are no equalities in ψ, there must exist two distinct points-to atoms $x \mapsto (t_1, \ldots, t_{\mathfrak{K}})$ and $y \mapsto (u_1, \ldots, u_{\mathfrak{K}})$ in ψ such that, $(\mathfrak{s}, \mathfrak{h}) \models_{\mathcal{S}_e} \phi$ implies $(\mathfrak{s}', \mathfrak{h}') \models_{\mathcal{S}_e} x \mapsto (t_1, \ldots, t_{\mathfrak{K}}) * y \mapsto (u_1, \ldots, u_{\mathfrak{K}})$, for any structure $(\mathfrak{s}, \mathfrak{h})$, for some heap $\mathfrak{h}' \subseteq \mathfrak{h}$ and $\mathfrak{s}'$ is a $(x_1, \ldots, x_n)$-associate of $\mathfrak{s}$. But then $(\mathfrak{s}', \emptyset) \models_{\mathcal{S}_e} x \neq y$ and, since the choice of the structure $(\mathfrak{s}, \mathfrak{h})$ was arbitrary, we can remove any disequality $x \neq y$ such that $\{x, y\} \cap C = \emptyset$ from $\mathcal{P}_e$. This transformation takes time $O(\mathrm{size}(\mathcal{P}_e)) = \mathrm{size}(\mathcal{P}) \cdot 2^{O(\mathrm{width}(\mathcal{P})^2)}$ and does not increase the width of the problem. The outcome of is an e-restricted entailment problem. ◀

D Additional Material for Normal Structures (Section 4)

▶ **Definition 34.** *Given symbolic heaps $\phi_1, \phi_2 \in \mathsf{SH}^{\mathfrak{K}}$, a pair of structures $\langle(\mathfrak{s}_1, \mathfrak{h}_1), (\mathfrak{s}_2, \mathfrak{h}_2)\rangle$ is a* normal $\mathcal{S}$-companion for (ϕ_1, ϕ_2) *iff $(\mathfrak{s}_i, \mathfrak{h}_i)$ is a normal $\mathcal{S}$-model of ϕ_i, for $i = 1, 2$ and:*

1. *$\overline{\mathfrak{s}}_1(t) = \overline{\mathfrak{s}}_2(t)$, for each term $t \in \mathsf{fv}(\psi_1) \cap \mathsf{fv}(\psi_2) \cup \mathbb{C}$,*
2. *$\overline{\mathfrak{s}}_i(\mathbf{x}_i) \cap \overline{\mathfrak{s}}_{3-i}(\mathsf{fv}(\psi_{3-i})) \subseteq \overline{\mathfrak{s}}_i(\mathbb{C})$, for $i = 1, 2$,*

where $\phi_i \Rightarrow^*_{\mathcal{S}} \exists \mathbf{x}_i \,.\, \psi_i$ are the predicate-free unfoldings and $\overline{\mathfrak{s}}_i$ is the $\mathbf{x}_i$-associate of $\mathfrak{s}_i$ satisfying conditions (1) and (2) of Definition 15, for $i = 1, 2$, respectively. The normal $\mathcal{S}$-companion $\langle(\mathfrak{s}_1, \mathfrak{h}_1), (\mathfrak{s}_2, \mathfrak{h}_2)\rangle$ is, moreover, injective *iff $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are injective and $\mathfrak{s}_1(\mathsf{fv}(\phi_1) \setminus \mathsf{fv}(\phi_2)) \cap \mathfrak{s}_2(\mathsf{fv}(\phi_2) \setminus \mathsf{fv}(\phi_1)) = \emptyset$.*

▶ **Lemma 35.** *Given symbolic heaps $\phi_1, \phi_2 \in \mathsf{SH}^{\Re}$, a structure $(\mathfrak{s}, \mathfrak{h})$ is a (injective) normal $\mathcal{S}$-model of $\phi_1 * \phi_2$ iff there exists a (injective) normal $\mathcal{S}$-companion $\langle(\mathfrak{s}_1, \mathfrak{h}_1), (\mathfrak{s}_2, \mathfrak{h}_2)\rangle$ for (ϕ_1, ϕ_2), such that $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$.*

Proof: "⇒" Let $(\mathfrak{s}, \mathfrak{h})$ be a normal $\mathcal{S}$-model of $\phi_1 * \phi_2$. Then there exists a predicate-free unfolding $\phi_1 * \phi_2 \Rightarrow^*_{\mathcal{S}} \exists \mathbf{x}_1 \,.\, \psi_1 * \exists \mathbf{x}_2 \,.\, \psi_2$ such that ψ_1 and ψ_2 are quantifier-free and $(\mathfrak{s}, \mathfrak{h}) \models \exists \mathbf{x}_1 \,.\, \psi_1 * \exists \mathbf{x}_2 \,.\, \psi_2$. By α-renaming if necessary, we can assume that $\mathbf{x}_i \cap \mathsf{fv}(\psi_{3-i}) = \emptyset$, for $i = 1, 2$, thus $(\mathfrak{s}, \mathfrak{h}) \models \exists \mathbf{x}_1 \exists \mathbf{x}_2 \,.\, \psi_1 * \psi_2$. Hence there exist an $(\mathbf{x}_1 \cup \mathbf{x}_2)$-associate $\overline{\mathfrak{s}}$ of $\mathfrak{s}$ and two disjoint heaps $\mathfrak{h}_1$ and $\mathfrak{h}_2$, such that $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$ and $(\overline{\mathfrak{s}}, \mathfrak{h}_i) \models \psi_i$, for $i = 1, 2$. Let $\mathfrak{s}_i \stackrel{\text{def}}{=} \mathfrak{s}$, for $i = 1, 2$, so that $\mathfrak{s} = \mathfrak{s}_1 \cup \mathfrak{s}_2$. By considering the $\mathbf{x}_i$-associate of $\mathfrak{s}$ defined as the restriction of $\overline{\mathfrak{s}}$ to $\mathbf{x}_i \cup \mathsf{dom}(\mathfrak{s})$ and using the fact that $(\mathfrak{s}, \mathfrak{h})$ is a normal $\mathcal{S}$-model of $\phi_1 * \phi_2$, it is easy to check that $(\mathfrak{s}_i, \mathfrak{h}_i)$ is a normal $\mathcal{S}$-model of ϕ_i. Further, points (1) and (2) of Definition 34 are easy checks. Finally, if $\mathfrak{s}$ is injective then trivially $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are injective and $\mathfrak{s}_1(\mathsf{trm}(\phi_1) \setminus \mathsf{trm}(\phi_2)) \cap \mathfrak{s}_2(\mathsf{trm}(\phi_2) \setminus \mathsf{trm}(\phi_1)) = \mathfrak{s}(\mathsf{trm}(\phi_1) \setminus \mathsf{trm}(\phi_2)) \cap \mathfrak{s}(\mathsf{trm}(\phi_2) \setminus \mathsf{trm}(\phi_1)) = \emptyset$.

"⇐" If $(\mathfrak{s}_i, \mathfrak{h}_i)$ is a normal $\mathcal{S}$-model of ϕ_i, then there exist predicate-free unfoldings $\phi_i \Rightarrow^*_{\mathcal{S}} \exists \mathbf{x}_i \,.\, \psi_i$ and $\mathbf{x}_i$-associates $\overline{\mathfrak{s}}_i$ of $\mathfrak{s}_i$, that satisfy the points (1) and (2) of Definition 15. By an α-renaming if necessary, we assume that $\mathbf{x}_1 \cap \mathbf{x}_2 = \emptyset$. Then $\phi_1 * \phi_2 \Rightarrow^*_{\mathcal{S}} \exists \mathbf{x}_1 \,.\, \psi_1 * \exists \mathbf{x}_2 \,.\, \psi_2$ is a predicate-free unfolding. Let $\mathfrak{s}'_i$ and $\overline{\mathfrak{s}}'_i$ be the restrictions of $\mathfrak{s}_i$ and $\overline{\mathfrak{s}}_i$ to $\mathsf{trm}(\phi_i)$ and $\mathsf{trm}(\psi_i)$ for $i = 1, 2$, respectively. By point (1) of Definition 34, $\mathfrak{s} \stackrel{\text{def}}{=} \mathfrak{s}'_1 \cup \mathfrak{s}'_2$ is a well-defined store and, since $\mathbf{x}_1 \cap \mathbf{x}_2 = \emptyset$, we obtain that $\overline{\mathfrak{s}} \stackrel{\text{def}}{=} \overline{\mathfrak{s}}'_1 \cup \overline{\mathfrak{s}}'_2$ is a well-defined $(\mathbf{x}_1 \cup \mathbf{x}_2)$-associate of $\mathfrak{s}$. To show that $(\mathfrak{s}, \mathfrak{h}_1 \uplus \mathfrak{h}_2)$ is a normal $\mathcal{S}$-model of $\phi_1 * \phi_2$, let $t_1, t_2 \in \mathsf{trm}(\psi_1) \cup \mathsf{trm}(\psi_2)$ be distinct terms such that $\overline{\mathfrak{s}}(t_1) = \overline{\mathfrak{s}}(t_2)$ and suppose, for a contradiction, that $\overline{\mathfrak{s}}(t_1) \notin \overline{\mathfrak{s}}(\mathbb{C})$. Since $(\mathfrak{s}_i, \mathfrak{h}_i)$ is a normal $\mathcal{S}$-model of ϕ_i, for $i = 1, 2$, the only interesting cases are $t_i \in \mathsf{trm}(\psi_i) \setminus \mathsf{trm}(\psi_{3-i})$ and $t_i \in \mathsf{trm}(\psi_{3-i}) \setminus \mathsf{trm}(\psi_i)$. Assume $t_i \in \mathsf{trm}(\psi_i) \setminus \mathsf{trm}(\psi_{3-i})$ for $i = 1, 2$, the other case is symmetric. Since $t_i \notin \mathsf{cst}(\psi_1 * \psi_2)$, it must be the case that $t_i \in \mathbf{x}_i$, for $i = 1, 2$. Then $\overline{\mathfrak{s}}_1(t_1) = \overline{\mathfrak{s}}(t_1) = \overline{\mathfrak{s}}(t_2) = \overline{\mathfrak{s}}_2(t_2)$, which contradicts point (2) of Definition 34. Finally, it is easy to check that $\mathfrak{s} = \mathfrak{s}'_1 \cup \mathfrak{s}'_2$ is injective, provided that $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are injective and that $\mathfrak{s}_1(\mathsf{trm}(\phi_1) \setminus \mathsf{trm}(\phi_2)) \cap \mathfrak{s}_2(\mathsf{trm}(\phi_2) \setminus \mathsf{trm}(\phi_1)) = \mathfrak{s}'_1(\mathsf{trm}(\phi_1) \setminus \mathsf{trm}(\phi_2)) \cap \mathfrak{s}'_2(\mathsf{trm}(\phi_2) \setminus \mathsf{trm}(\phi_1)) = \emptyset$. ◀

The following lemma states an important property of normal $\mathcal{S}$-models, that will be used to build abstract composition operators, needed to define a finite-range abstraction of an infinite set normal structures.

▶ **Lemma 36.** *Given symbolic heaps $\phi_1, \phi_2 \in \mathsf{SH}^{\Re}$ and $\langle(\dot{\mathfrak{s}}, \mathfrak{h}_1), (\dot{\mathfrak{s}}, \mathfrak{h}_2)\rangle$ an injective normal $\mathcal{S}$-companion for (ϕ_1, ϕ_2), we have* $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \subseteq \dot{\mathfrak{s}}(\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C})$.

Proof: Let $\ell \in \mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) = \mathrm{loc}(\mathfrak{h}_1) \cap \mathrm{loc}(\mathfrak{h}_2)$ be a location, $\phi_i \Rightarrow^*_{\mathcal{S}} \exists \mathbf{x}_i \,.\, \psi_i$ be predicate-free unfoldings and $\overline{\mathfrak{s}}_i$ be the $\mathbf{x}_i$-associates of $\dot{\mathfrak{s}}$ that satisfy points (1) and (2) of Definition 34, such that $(\overline{\mathfrak{s}}_i, \mathfrak{h}_i) \models \psi_i$, for $i = 1, 2$. By α-renaming, if necessary, we assume w.l.o.g. that $\mathbf{x}_i \cap \mathsf{fv}(\psi_{3-i}) = \emptyset$, for $i = 1, 2$. Because $\ell \in \mathrm{loc}(\mathfrak{h}_i)$, there exist points-to atoms $t^i_0 \mapsto (t^i_1, \ldots, t^i_{\Re})$ in ψ_i, such that $\ell = \overline{\mathfrak{s}}_1(t^1_{i_1}) = \overline{\mathfrak{s}}_2(t^2_{i_2})$, for some $i_1, i_2 \in [\![0 \,..\, \Re]\!]$ and all $i = 1, 2$. We distinguish two cases:

- if $t^1_{i_1} \in \mathsf{trm}(\phi_1)$ and $t^2_{i_2} \in \mathsf{trm}(\phi_2)$, since $\overline{\mathfrak{s}}_i$ is a $\mathbf{x}_i$-associate of $\dot{\mathfrak{s}}$, $\overline{\mathfrak{s}}_i$ and $\dot{\mathfrak{s}}$ agree over $\mathsf{trm}(\phi_i)$, for $i = 1, 2$, we obtain $\dot{\mathfrak{s}}(t^1_{i_1}) = \overline{\mathfrak{s}}_1(t^1_{i_1}) = \overline{\mathfrak{s}}_2(t^2_{i_2}) = \dot{\mathfrak{s}}(t^2_{i_2})$, thus $t^1_{i_1} = t^2_{i_2}$, because $\dot{\mathfrak{s}}$ is injective, hence $\ell \in \dot{\mathfrak{s}}(\mathsf{trm}(\phi_1) \cap \mathsf{trm}(\phi_2)) \subseteq \dot{\mathfrak{s}}(\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C})$.
- else $t^1_{i_1} \in \mathsf{trm}(\psi_1) \setminus \mathsf{trm}(\phi_1) = \mathbf{x}_1 \cup \mathbb{C}$ (the case $t^2_{i_2} \in \mathsf{trm}(\psi_2) \setminus \mathsf{trm}(\phi_2)$ is symmetric). If $t^1_{i_1} \in \mathbb{C}$, we obtain $\ell = \overline{\mathfrak{s}}_1(t^1_{i_1}) = \dot{\mathfrak{s}}(t^1_{i_1}) \in \dot{\mathfrak{s}}(\mathbb{C})$, because $\mathbb{C} \subseteq \mathsf{dom}(\dot{\mathfrak{s}})$ and $\overline{\mathfrak{s}}$ agrees with $\dot{\mathfrak{s}}$ over $\mathbb{C}$. Else $t^1_{i_1} \in \mathbf{x}_1$ and we distinguish two cases:
  - if $t^2_{i_2} \in \mathsf{cst}(\psi_2)$, we obtain $\ell = \dot{\overline{\mathfrak{s}}}_2(t^2_{i_2}) = \dot{\mathfrak{s}}(t^2_{i_2}) \in \dot{\mathfrak{s}}(\mathbb{C})$, by the above argument.
  - else $t^2_{i_2} \in \mathsf{fv}(\psi_2)$ and $\overline{\mathfrak{s}}_1(t^1_{i_1}) = \overline{\mathfrak{s}}_2(t^2_{i_2}) \in \overline{\mathfrak{s}}(\mathbb{C})$ by point (2) of Definition 34. ◀

▶ **Example 37.** Consider the structures defined in Example 16. The structure $(\mathfrak{s}, \mathfrak{h})$ is a normal model of $p(x_1) * p(x_2)$: we have $(\mathfrak{s}, \mathfrak{h}_i) \models p(x_i)$ with $\mathfrak{h}_i = (\ell_i \mapsto \ell_3)$ (for $i = 1, 2$), $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$ and $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) = \{\ell_3\} \subseteq \dot{\mathfrak{s}}(\mathbb{C})$. Similarly, $(\mathfrak{s}, \mathfrak{h}')$ is a normal model of $p(x_1) * p(x_2)$, $(\mathfrak{s}, \mathfrak{h}'_i) \models p(x_i)$ with

$\mathfrak{h}'_i = (\ell_i \mapsto \ell_{3+i})$ (for $i = 1,2$), $\mathfrak{h}' = \mathfrak{h}'_1 \uplus \mathfrak{h}'_2$ and $\mathrm{Fr}(\mathfrak{h}'_1, \mathfrak{h}'_2) = \emptyset$. On the other hand, $(\mathfrak{s}, \mathfrak{h}'')$ is not normal: we have $(\mathfrak{s}, \mathfrak{h}''_i) \models p(x_i)$ with $\mathfrak{h}''_i = (\ell_i \mapsto \ell_4)$ (for $i = 1,2$), $\mathfrak{h}'' = \mathfrak{h}''_1 \uplus \mathfrak{h}''_2$ and $\mathrm{Fr}(\mathfrak{h}''_1, \mathfrak{h}''_2) = \{\ell_4\} \not\subseteq \mathfrak{s}(\mathsf{fv}(p(x_1)) \cap \mathsf{fv}(p(x_2)) \cup \mathbb{C}) = \{\ell_3\}$.

The proof of this result (Lemma 17) relies on the following definition and lemmas.

▶ **Definition 38.** *A total function $\gamma : \mathbb{L} \to \mathbb{L}$ is* compatible *with a structure $(\mathfrak{s}, \mathfrak{h})$ if and only if, for all $\ell_1, \ell_2 \in \mathbb{L}$ such that either $\ell_1, \ell_2 \in \mathrm{dom}(\mathfrak{h})$ or $\ell_1 \in \mathfrak{s}(\mathbb{C})$, if $\gamma(\ell_1) = \gamma(\ell_2)$ then $\ell_1 = \ell_2$. We define $\gamma(\mathfrak{h}) \stackrel{\text{def}}{=} \{\langle \gamma(\ell), (\gamma(\ell_1), \ldots, \gamma(\ell_{\mathfrak{K}}))\rangle \mid \mathfrak{h}(\ell) = (\ell_1, \ldots, \ell_{\mathfrak{K}})\}$, whenever γ is compatible with $(\mathfrak{s}, \mathfrak{h})$.*

▶ **Lemma 39.** *Let $\mathcal{S}$ be an e-restricted (resp. normalized) set of rules and ϕ be an e-restricted formula. Then, each unfolding ψ of ϕ is e-restricted (resp. normalized).*

Proof: The proof is by induction on the length of the unfolding sequence $\phi \Rightarrow^*_{\mathcal{S}} \psi$. ◀

▶ **Lemma 40.** *If $\mathcal{S}$ is an e-restricted set of rules, ϕ is an e-restricted formula and $(\mathfrak{s}, \mathfrak{h})$ is an $\mathcal{S}$-model of ϕ, then for any total function γ compatible with $(\mathfrak{s}, \mathfrak{h})$, the following hold: (1) $\gamma(\mathfrak{h})$ is a heap, (2) $(\gamma \circ \mathfrak{s}, \gamma(\mathfrak{h})) \models_{\mathcal{S}} \phi$.*

Proof: (1) The set $\{\gamma(\ell) \mid \ell \in \mathrm{dom}(\mathfrak{h})\}$ is finite, because $\mathrm{dom}(\mathfrak{h})$ is finite. Consider two tuples $\langle \gamma(\ell), (\gamma(\ell_1), \ldots, \gamma(\ell_{\mathfrak{K}}))\rangle$ and $\langle \gamma(\ell'), (\gamma(\ell'_1), \ldots, \gamma(\ell'_{\mathfrak{K}}))\rangle \in \gamma(\mathfrak{h})$ and assume that $\gamma(\ell) = \gamma(\ell')$. Then since γ is compatible with $(\mathfrak{s}, \mathfrak{h})$, necessarily $\ell = \ell'$. Since $\mathfrak{h}$ is a partial function, we have $(\ell_1, \ldots, \ell_{\mathfrak{K}}) = (\ell'_1, \ldots, \ell'_{\mathfrak{K}})$, so that $\gamma(\mathfrak{h})$ is also a finite partial function.
(2) If $(\mathfrak{s}, \mathfrak{h}) \models_{\mathcal{S}} \phi$ then there exists a predicate-free unfolding $\phi \Rightarrow_{\mathcal{S}} \psi = \exists \mathbf{x} \,.\, \ast^n_{i=1} t_i \simeq u_i * \ast^m_{i=1} t'_i \neq u'_i * \ast^k_{i=1} x_i \mapsto (t^i_1, \ldots, t^i_{\mathfrak{K}})$, such that $(\overline{\mathfrak{s}}, \mathfrak{h}) \models \psi$, for an $\mathbf{x}$-associate $\overline{\mathfrak{s}}$ of $\mathfrak{s}$. Note that $\gamma \circ \overline{\mathfrak{s}}$ is an $\mathbf{x}$-associate of $\gamma \circ \mathfrak{s}$, because γ is total. Moreover, because ϕ and $\mathcal{S}$ are both e-restricted, by Lemma 39, ψ is e-restricted, thus we can assume that $t_i \in \mathbb{C}$, for all $i \in [\![1 \,..\, n]\!]$ and that $t'_i \in \mathbb{C}$, for all $i \in [\![1 \,..\, m]\!]$. We consider the three types of atoms from ψ below:

- For any $i \in [\![1 \,..\, n]\!]$, since $(\overline{\mathfrak{s}}, \emptyset) \models t_i \simeq u_i$, we have $\overline{\mathfrak{s}}(t_i) = \overline{\mathfrak{s}}(u_i)$, thus $\gamma(\overline{\mathfrak{s}}(t_i)) = \gamma(\overline{\mathfrak{s}}(s_i))$, leading to $(\gamma \circ \overline{\mathfrak{s}}, \emptyset) \models t_i \simeq u_i$.
- For any $i \in [\![1 \,..\, m]\!]$, since $(\overline{\mathfrak{s}}, \emptyset) \models t'_i \neq u'_i$, we have $\overline{\mathfrak{s}}(t'_i) \neq \overline{\mathfrak{s}}(u'_i)$. Because $t'_i \in \mathbb{C}$ and $(\mathfrak{s}, \mathfrak{h}) \models \phi$, we have $t'_i \in \mathrm{dom}(\mathfrak{s})$ and $\overline{\mathfrak{s}}(t'_i) = \mathfrak{s}(t'_i) \in \mathfrak{s}(\mathbb{C})$. By Definition 38, we obtain $\gamma(\overline{\mathfrak{s}}(t'_i)) \neq \gamma(\overline{\mathfrak{s}}(u'_i))$, thus $(\gamma \circ \overline{\mathfrak{s}}, \emptyset) \models t'_i \neq u'_i$.
- If $(\overline{\mathfrak{s}}, \mathfrak{h}) \models \ast^k_{i=1} x_i \mapsto (t^i_1, \ldots, t^i_{\mathfrak{K}})$ then $\overline{\mathfrak{s}}(x_1), \ldots, \overline{\mathfrak{s}}(x_k)$ are pairwise distinct and $\mathrm{dom}(\mathfrak{h}) = \{\overline{\mathfrak{s}}(x_1), \ldots, \overline{\mathfrak{s}}(x_k)\}$. Since $\overline{\mathfrak{s}}(x_1), \ldots, \overline{\mathfrak{s}}(x_k) \in \mathrm{dom}(\mathfrak{h})$, by Definition 38, we obtain that $\gamma(\overline{\mathfrak{s}}(x_1)), \ldots, \gamma(\overline{\mathfrak{s}}(x_k))$ are pairwise distinct and $\mathrm{dom}(\gamma(\mathfrak{h})) = \{\gamma(\overline{\mathfrak{s}}(x_1)), \ldots, \gamma(\overline{\mathfrak{s}}(x_k))\}$. We have $\mathfrak{h}(\overline{\mathfrak{s}}(x_i)) = (\overline{\mathfrak{s}}(t^i_1), \ldots, \overline{\mathfrak{s}}(t^i_{\mathfrak{K}}))$, thus $\gamma(\mathfrak{h})(\overline{\mathfrak{s}}(x_i)) = (\gamma(\overline{\mathfrak{s}}(t^i_1)), \ldots, \gamma(\overline{\mathfrak{s}}(t^i_{\mathfrak{K}})))$, for each $i \in [\![1 \,..\, k]\!]$, by Definition 38 and $(\gamma \circ \overline{\mathfrak{s}}, \gamma(\mathfrak{h})) \models \ast^k_{i=1} x_i \mapsto (t^i_1, \ldots, t^i_{\mathfrak{K}})$. ◀

E Proof of Lemma 17 (Section 4)

This direction is trivial. "⇐" Let $(\dot{\mathfrak{s}}, \mathfrak{h})$ be an injective $\mathcal{S}$-model of ϕ. Then by Lemma 39, there exists a predicate-free unfolding $\phi \Rightarrow^*_{\mathcal{S}} \exists \mathbf{x} \,.\, \varphi$, where $\varphi = \ast^m_{i=1} t_i \neq u_i * \ast^k_{i=1} x_i \mapsto (t^i_1, \ldots, t^i_{\mathfrak{K}})$ is e-restricted and normalized, and an $\mathbf{x}$-associate $\overline{\mathfrak{s}}$ of $\dot{\mathfrak{s}}$ such that $(\overline{\mathfrak{s}}, \mathfrak{h}) \models \varphi$. Note that φ contains no equalities since it is normalized and, since it is e-restricted, we can assume that $t_i \in \mathbb{C}$, for all $i \in [\![1 \,..\, m]\!]$. We consider a store $\mathfrak{s}' : \mathrm{dom}(\overline{\mathfrak{s}}) \to \mathbb{L}$ that satisfies the following hypothesis:
(a) $\mathfrak{s}'(t) = \overline{\mathfrak{s}}(t)$, for each $t \in \mathrm{dom}(\overline{\mathfrak{s}})$ such that $\overline{\mathfrak{s}}(t) \in \overline{\mathfrak{s}}(\mathbb{C})$,
(b) $\mathfrak{s}'(t) \neq \mathfrak{s}'(u)$, for all terms $t \neq u \in \mathrm{dom}(\overline{\mathfrak{s}})$ such that $\overline{\mathfrak{s}}(t) \notin \overline{\mathfrak{s}}(\mathbb{C})$ or $\overline{\mathfrak{s}}(u) \notin \overline{\mathfrak{s}}(\mathbb{C})$.
Note that such a store exists because $\mathbb{L}$ is infinite, thus all terms that are not already mapped by $\overline{\mathfrak{s}}$ into locations from $\overline{\mathfrak{s}}(\mathbb{C})$ can be mapped to pairwise distinct locations, not occurring in $\overline{\mathfrak{s}}(\mathbb{C})$. Then we define

the heap $\mathfrak{h}' \stackrel{\text{def}}{=} \{\langle \mathfrak{s}'(x_i), (\mathfrak{s}'(t_1^i), \ldots, \mathfrak{s}'(t_{\Re}^i))\rangle \mid i \in [\![1 \,..\, k]\!]\}$. To prove that $\mathfrak{h}'$ is a well-defined heap, first note that the set $\{\mathfrak{s}'(x_i) \mid i \in [\![1 \,..\, k]\!]\}$ is finite and suppose, for a contradiction that $\mathfrak{s}'(x_i) = \mathfrak{s}'(x_j)$, for some $i \neq j \in [\![1 \,..\, k]\!]$. By point (b), it must be the case that $\overline{\mathfrak{s}}(x_i), \overline{\mathfrak{s}}(x_j) \in \overline{\mathfrak{s}}(\mathbb{C})$, in which case we obtain $\overline{\mathfrak{s}}(x_i) = \mathfrak{s}'(x_i) = \mathfrak{s}'(x_j) = \overline{\mathfrak{s}}(x_j)$, by point (a), thus contradicting the fact that $(\overline{\mathfrak{s}}, \mathfrak{h}) \models \mathbin{\ast}_{i=1}^{k} x_i \mapsto (t_1^i, \ldots, t_{\Re}^i)$. Hence the locations $\{\mathfrak{s}'(x_i) \mid i \in [\![1 \,..\, k]\!]\}$ are pairwise distinct and $\mathfrak{h}'$ is a finite partial function. We prove next that $(\mathfrak{s}', \mathfrak{h}') \models \varphi$, considering each type of atom in φ:

- for any $i \in [\![1 \,..\, m]\!]$, since $(\overline{\mathfrak{s}}, \emptyset) \models t_i \neq u_i$, we have $\overline{\mathfrak{s}}(t_i) \neq \overline{\mathfrak{s}}(u_i)$ and, since $t_i \in \mathbb{C}$, we obtain $\mathfrak{s}'(t_i) = \overline{\mathfrak{s}}(t_i) \in \overline{\mathfrak{s}}(\mathbb{C})$. We distinguish the following cases:
  - if $\overline{\mathfrak{s}}(u_i) \in \overline{\mathfrak{s}}(\mathbb{C})$ then $\mathfrak{s}'(u_i) = \overline{\mathfrak{s}}(u_i) \neq \overline{\mathfrak{s}}(t_i) = \mathfrak{s}'(t_i)$, by point (a),
  - otherwise, $\overline{\mathfrak{s}}(u_i) \notin \overline{\mathfrak{s}}(\mathbb{C})$ and $\mathfrak{s}'(t_i) \neq \mathfrak{s}'(u_i)$, by point (b).

  In both cases, we have $(\mathfrak{s}', \emptyset) \models t_i \neq u_i$.
- $(\mathfrak{s}', \mathfrak{h}') \models \mathbin{\ast}_{i=1}^{k} x_i \mapsto (t_1^i, \ldots, t_{\Re}^i)$, by the definition of $\mathfrak{h}'$.

Let $\mathfrak{s}''$ be the restriction of $\mathfrak{s}'$ to $\mathrm{dom}(\dot{\mathfrak{s}})$. By point (b), $(\mathfrak{s}'', \mathfrak{h}')$ is an injective normal $\mathcal{S}$-model of ϕ, according to Definition 15 (simply let $\mathfrak{s}'$ be its $\mathbf{x}$-associate). Because $\mathfrak{s}''$ is injective, by the assumption of the Lemma, we obtain $(\mathfrak{s}'', \mathfrak{h}') \models_{\mathcal{S}} \psi_i$, for some $i \in [\![1 \,..\, n]\!]$, and we are left with proving the sufficient condition $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathcal{S}} \psi_i$. To this end, consider the function $\gamma : \mathbb{L} \to \mathbb{L}$, defined as:

- $\gamma(\mathfrak{s}''(x)) = \overline{\mathfrak{s}}(x)$, for all $x \in \mathrm{dom}(\mathfrak{s}'')$,
- $\gamma(\ell) = \ell$, for all $\ell \in \mathbb{L} \setminus \mathrm{rng}(\mathfrak{s}'')$.

Observe that γ is well-defined, since by definition of $\mathfrak{s}'$, $\mathfrak{s}'(x) = \mathfrak{s}'(x') \Rightarrow \overline{\mathfrak{s}}(x) = \overline{\mathfrak{s}}(x')$. Below we check that γ is compatible with $(\mathfrak{s}'', \mathfrak{h}')$. Let $\ell_1, \ell_2 \in \mathbb{L}$ be two locations such that $\gamma(\ell_1) = \gamma(\ell_2)$:

- if $\ell_1, \ell_2 \in \mathrm{dom}(\mathfrak{h}')$ then $\ell_1 = \mathfrak{s}''(x_i)$ and $\ell_2 = \mathfrak{s}''(x_j)$, for some $i, j \in [\![1 \,..\, k]\!]$, by definition of $\mathfrak{h}'$. Suppose, for a contradiction, that $i \neq j$. Then $\overline{\mathfrak{s}}(x_i) = \gamma(\mathfrak{s}''(x_i)) = \gamma(\mathfrak{s}''(x_j)) = \overline{\mathfrak{s}}(x_j)$, which contradicts the fact that $(\overline{\mathfrak{s}}, \mathfrak{h}) \models \mathbin{\ast}_{i=1}^{k} x_i \mapsto (t_1^i, \ldots, t_{\Re}^i)$. Hence $i = j$, leading to $\ell_1 = \ell_2$.
- if $\ell_1 \in \mathfrak{s}''(\mathbb{C})$, then let $c \in \mathbb{C}$ be a constant such that $\ell_1 = \mathfrak{s}''(c)$, so that $\gamma(\ell_1) = \overline{\mathfrak{s}}(c)$. Suppose, for a contradiction, that $\ell_2 \notin \mathrm{rng}(\mathfrak{s}'')$. Then $\gamma(\ell_2) = \ell_2 = \overline{\mathfrak{s}}(c)$, hence $\ell_2 \in \overline{\mathfrak{s}}(\mathbb{C})$. But since $\overline{\mathfrak{s}}$ and $\mathfrak{s}''$ agree over $\mathbb{C}$, we have $\overline{\mathfrak{s}}(c) \in \mathfrak{s}''(\mathbb{C})$. Hence $\ell_2 = \overline{\mathfrak{s}}(c) = \mathfrak{s}''(c)$, which contradicts with $\ell_2 \notin \mathrm{rng}(\mathfrak{s}'')$. Thus $\ell_2 \in \mathrm{rng}(\mathfrak{s}'')$ and let $\ell_2 = \mathfrak{s}''(t)$, for some term t. We have $\gamma(\mathfrak{s}''(t)) = \overline{\mathfrak{s}}(t)$, thus $\overline{\mathfrak{s}}(c) = \gamma(\ell_2) = \gamma(\ell_1) = \overline{\mathfrak{s}}(t)$. By point (a), we obtain $\ell_2 = \mathfrak{s}'(t) = \overline{\mathfrak{s}}(t) = \overline{\mathfrak{s}}(c) = \mathfrak{s}''(c) = \ell_1$.

Moreover, it is easy to check that $(\overline{\mathfrak{s}}, \mathfrak{h}) = (\gamma \circ \mathfrak{s}'', \gamma(\mathfrak{h}'))$. Since $\dot{\mathfrak{s}}$ is the restriction of $\overline{\mathfrak{s}}$ to $\mathsf{trm}(\phi)$, by Lemma 40, we obtain $(\dot{\mathfrak{s}}, \mathfrak{h}) \models \psi_i$. ◀

F Additional Material on Core Formulæ (Section 5)

The formal semantics of the bounded quantifiers is stated below:

▶ **Lemma 41.** *Given a* $\mathsf{SL}^{\Re}$ *formula* ϕ *and* $x \in \mathsf{fv}(\phi)$*, the following hold, for any structure* $(\mathfrak{s}, \mathfrak{h})$*:*

1. $(\mathfrak{s}, \mathfrak{h}) \models_{\mathcal{S}} \exists_{\mathsf{h}} x \,.\, \phi$ *iff* $(\mathfrak{s}[x \leftarrow \ell], \mathfrak{h}) \models_{\mathcal{S}} \phi$*, for some* $\ell \in \mathrm{loc}(\mathfrak{h}) \setminus \mathfrak{s}((\mathsf{fv}(\phi) \setminus \{x\}) \cup \mathbb{C})$,
2. $(\mathfrak{s}, \mathfrak{h}) \models_{\mathcal{S}} \forall_{\neg \mathsf{h}} x \,.\, \phi$ *iff* $(\mathfrak{s}[x \leftarrow \ell], \mathfrak{h}) \models_{\mathcal{S}} \phi$*, for all* $\ell \in \mathbb{L} \setminus [\mathrm{loc}(\mathfrak{h}) \cup \mathfrak{s}((\mathsf{fv}(\phi) \setminus \{x\}) \cup \mathbb{C})]$.

Proof: First, for any structure $(\mathfrak{s}, \mathfrak{h})$, we have $(\mathfrak{s}, \mathfrak{h}) \models \mathsf{loc}(x) \Leftrightarrow \mathfrak{s}(x) \in \mathrm{loc}(\mathfrak{h})$.
(1) By definition, $\exists_{\mathsf{h}} x \,.\, \phi$ is equivalent to $\exists x \,.\, \bigwedge_{t \in (\mathsf{fv}(\phi) \setminus \{x\}) \cup \mathbb{C}} \neg x \approx y \wedge \mathsf{loc}(x) \wedge \phi$.
(2) By definition, $\forall_{\neg \mathsf{h}} x \,.\, \phi$ is equivalent to $\forall x \,.\, (\bigwedge_{t \in (\mathsf{fv}(\phi) \setminus \{x\}) \cup \mathbb{C}} \neg x \approx t \wedge \neg \mathsf{loc}(x)) \rightarrow \phi$. ◀
Below we prove the equivalence between the atoms $p(\mathbf{t})$ and $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$.

▶ **Lemma 42.** *A structure* $(\mathfrak{s}, \mathfrak{h})$ *is an* $\mathcal{S}$*-model of* $p(\mathbf{t})$ *if and only if* $(\mathfrak{s}, \mathfrak{h})$ *is a* $\mathfrak{C}_{\mathcal{S}}$*-model of* $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$.

Proof: "⇒" For each rule $p(\mathbf{x}) \Leftarrow_{\mathcal{S}} \exists \mathbf{z} \,.\, \psi \mathbin{\ast} \mathbin{\ast}_{i=1}^{n} q_i(\mathbf{y}_i)$, there exists a rule $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{z} \,.\, \psi \mathbin{\ast} \mathbin{\ast}_{i=1}^{n} \mathsf{emp} \mathrel{-\!\!\bullet} q_i(\mathbf{y}_i)$, corresponding to the case where the substitution σ is empty. The proof follows by a simple induction on the length of the predicate-free unfolding of $p(\mathbf{t})$. "⇐" We prove the other direction by induction on the length of the predicate-free unfolding of $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$. Assume $(\mathfrak{s}, \mathfrak{h})$ is a $\mathfrak{C}_{\mathcal{S}}$-model of $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$. Then there exist a rule $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{v} \,.\, \psi\sigma \mathbin{\ast} \mathbin{\ast}_{j=1}^{m} \left(\mathsf{emp} \mathrel{-\!\!\bullet} p_j(\sigma(\mathbf{w}_j))\right)$

in $\mathfrak{C}_{\mathcal{P}}$ and a $\mathbf{v}$-associate $\mathfrak{s}'$ of $\mathfrak{s}$ such that $(\mathfrak{s}', \mathfrak{h}) \models \psi\sigma\theta * \circledast_{j=1}^{m} \Big(\mathsf{emp} \mathrel{-\!\!\bullet} p_j(\theta \circ \sigma(\mathbf{w}_j))\Big)$. By definition of $\mathfrak{C}_{\mathcal{P}}$, this entails that $p(\mathbf{t})$ can be unfolded into $\exists \mathbf{z} \,.\, \psi\theta * \circledast_{j=1}^{m} p_j(\theta(\mathbf{w}_j))$ using the rules in $\mathcal{S}$. The heap $\mathfrak{h}$ can be decomposed into $\mathfrak{h}_0 \uplus \cdots \uplus \mathfrak{h}_m$, where $(\mathfrak{s}', \mathfrak{h}_j) \models \mathsf{emp} \mathrel{-\!\!\bullet} p_j(\theta \circ \sigma(\mathbf{w}_j))$, for $j \in [\![1 \,..\, m]\!]$. By the induction hypothesis, $(\mathfrak{s}', \mathfrak{h}_j)$ is an $\mathcal{S}$-model of $p_j(\theta \circ \sigma(\mathbf{w}_j))$, and we deduce that $(\mathfrak{s}, \mathfrak{h})$ is an $\mathcal{S}$-model of $\exists \mathbf{z} \,.\, \psi\theta * \circledast_{j=1}^{m} p_j(\theta(\mathbf{w}_j))$. ◀

Another property of context predicate atoms is stated by the lemma below:

▶ **Lemma 43.** *If $\mathcal{S}$ is progressing, then for each store (resp. injective store) $\mathfrak{s}$, we have $(\mathfrak{s}, \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$ if and only if $n = 1$, $p = q_1$ and $\mathfrak{s}(\mathbf{t}) = \mathfrak{s}(\mathbf{u}_1)$ (resp. $\mathbf{t} = \mathbf{u}_1$).*

Proof: "⇒" If $(\mathfrak{s}, \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$ then there exists a rule $\circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \phi$ and a substitution σ such that $(\mathfrak{s}, \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \phi\sigma$, where $\sigma = [\mathbf{t}/\mathbf{x}, \mathbf{u}_1/\mathbf{y}_1, \ldots, \mathbf{u}_n/\mathbf{y}_n]$. If the rule is an instance of (I) then $n = 1$, $p = q_1$ and $(\mathfrak{s}, \emptyset) \models \mathbf{t} \doteq \mathbf{u}_1$, leading to $\mathfrak{s}(\mathbf{t}) = \mathfrak{s}(\mathbf{u}_1)$. If, moreover $\mathfrak{s}$ is injective, we get $\mathbf{t} = \mathbf{u}_1$. Otherwise, if the rule is an instance of (II), then since $\mathcal{S}$ is progressing, $\phi\sigma$ must contain exactly one points-to atom, hence $(\mathfrak{s}, \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \phi\sigma$ cannot be the case. "⇐" This is a simple application of rule (I). ◀

The following lemma states a technical result about core formulæ, that will be used in the proof of Lemma 30:

▶ **Lemma 44.** *For each quantifier-free core formula φ, each injective $\mathfrak{C}_{\mathcal{S}}$-model $(\dot{\mathfrak{s}}, \mathfrak{h})$ of φ such that $\|\mathfrak{h}\| \geq 1$, and each term $t \in \mathrm{roots}_{\mathsf{lhs}}(\varphi)$, we have $\dot{\mathfrak{s}}(t) \in \mathrm{loc}(\mathfrak{h}) \cup \dot{\mathfrak{s}}(\mathbb{C})$.*

Proof: Let φ be a quantifier-free core formula of the following form (cf. Definition 19):

$$\circledast_{i=1}^{n} \left(\circledast_{j=1}^{k_i} q_j^i(\mathbf{u}_j^i) \mathrel{-\!\!\bullet} p_i(\mathbf{t}_i) \right) * \circledast_{i=n+1}^{m} x_i \mapsto (t_1^i, \ldots, t_{\aleph}^i) \tag{12}$$

The proof goes by induction on $\|\mathfrak{h}\|$. In the base case, $\|\mathfrak{h}\| = 1$, we prove first that the formula contains exactly one points-to or predicate atom. Suppose, for a contradiction, that it contains two or more atoms, i.e. $\varphi = \alpha_1 * \ldots * \alpha_m$, for $m \geq 2$. If α_1 and α_2 are points-to atoms, it cannot be the case that $(\dot{\mathfrak{s}}, \mathfrak{h})$ is a $\mathfrak{C}_{\mathcal{S}}$-model of φ, thus we distinguish two cases:

- If $\alpha_1 = \circledast_{j=1}^{k} q_j(\mathbf{u}_j) \mathrel{-\!\!\bullet} p(\mathbf{t})$ and α_2 is a points-to atom then, since $\|\mathfrak{h}\| = 1$, we must have $(\dot{\mathfrak{s}}, \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \alpha_1$ and $(\dot{\mathfrak{s}}, \mathfrak{h}) \models \alpha_2$. By Lemma 43, we obtain $k = 1$ and $q_1(\mathbf{u}_1) = p(\mathbf{t})$, which violates the condition on the uniqueness of roots in $q_1(\mathbf{u}_1) \mathrel{-\!\!\bullet} p(\mathbf{t})$, in Definition 19.
- Otherwise, α_1 and α_2 are both predicate atoms; we assume that $(\dot{\mathfrak{s}}, \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \alpha_1$ (the case $(\dot{\mathfrak{s}}, \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \alpha_2$ is identical). We obtain a contradiction by the argument used at the previous point.

If φ consists of a single points-to atom, then $\mathrm{roots}_{\mathsf{lhs}}(\varphi) = \emptyset$ and there is nothing to prove. Otherwise, φ is of the form $\alpha_1 = \circledast_{i=1}^{k} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$. By Lemma 43, since $\mathcal{S}$ is progressing and $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \circledast_{i=1}^{k} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$, either $k > 1$ or $k = 1$ and $q_1(\mathbf{u}_1) \neq p(\mathbf{t})$. By Condition (II), there exists:

(a) a rule $p(\mathbf{x}) \Leftarrow_{\mathcal{S}} \exists \mathbf{z} \,.\, \psi * \circledast_{j=1}^{m} p_j(\mathbf{w}_j)$,

(b) separating conjunctions of predicate atoms $\gamma_1, \ldots, \gamma_m$, such that $\circledast_{j=1}^{m} \gamma_j = \circledast_{i=1}^{k} q_i(\mathbf{y}_i)$,

(c) a substitution $\tau : \mathbf{z} \rightharpoonup \mathbf{x} \cup \bigcup_{i=1}^{n} \mathbf{y}_i$,

that induce the rule:

$$\circledast_{i=1}^{k} q_i(\mathbf{y}_i) \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{v} \,.\, \psi\tau * \circledast_{j=1}^{m} \gamma_j \mathrel{-\!\!\bullet} p_j(\tau(\mathbf{w}_j)),$$

where $\mathbf{v} = \mathbf{z} \setminus \mathrm{dom}(\tau)$. Assume w.l.o.g. that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \circledast_{i=1}^{k} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$ is the consequence of the above rule, meaning that:

$$(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \Big(\exists \mathbf{v} \,.\, \psi\tau * \circledast_{j=1}^{m} \big(\gamma_j \mathrel{-\!\!\bullet} p_j(\tau(\mathbf{w}_j)) \big) \Big) \sigma, \text{ where } \sigma = [\mathbf{t}/\mathbf{x}, \mathbf{u}_1/\mathbf{y}_1, \ldots, \mathbf{u}_n/\mathbf{y}_n].$$

Let $\bar{\mathfrak{s}}$ be the $\mathbf{v}$-associate of $\dot{\mathfrak{s}}$ such that $(\bar{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \psi\tau\sigma * \circledast_{j=1}^{m} \big(\gamma_j\sigma \mathrel{-\!\!\bullet} p_j(\sigma(\tau(\mathbf{w}_j))) \big)$. Since $\mathcal{S}$ is progressing, ψ contains a points-to atom $t_0 \mapsto (t_1, \ldots, t_{\aleph})$, such that $(\bar{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} (t_0 \mapsto (t_1, \ldots, t_{\aleph}))\tau\sigma$ and

$(\bar{\mathfrak{s}}, \emptyset) \models_{\mathfrak{C}_\mathcal{S}} \ast_{j=1}^{m} \big(\gamma_j\sigma \mathrel{-\!\!\bullet} p_j(\sigma(\tau(\mathbf{w}_j)))\big)$. Now consider $t \in \mathsf{roots}_{\mathsf{lhs}}(\phi)$, then $t = \mathsf{root}(q_i(\mathbf{u}_i))$, for some $i \in [\![1 \,..\, k]\!]$. Since $\ast_{j=1}^{m} \gamma_j\sigma = \ast_{i=1}^{k} q_i(\mathbf{u}_i)$ by Condition (b), we have $t \in \mathsf{trm}(\gamma_j\sigma)$, for some $j \in [\![1 \,..\, m]\!]$. Since $(\bar{\mathfrak{s}}, \emptyset) \models_{\mathfrak{C}_\mathcal{S}} \gamma_j\sigma \mathrel{-\!\!\bullet} p_j(\sigma(\tau(\mathbf{w}_j)))$, by Lemma 43, we have $\bar{\mathfrak{s}}(t) = \bar{\mathfrak{s}}(\sigma(\tau(r)))$, where $r = \mathsf{root}(p_j(\mathbf{w}_j))$. Since $\mathcal{S}$ is connected, either $r \in \{t_1, \ldots, t_\mathfrak{K}\}$ or $r \in \mathbb{C}$, by Definition 5. Since $t \in \mathsf{roots}_{\mathsf{lhs}}(\phi)$, we have $\bar{\mathfrak{s}}(t) = \dot{\mathfrak{s}}(t)$, and we conclude that $\dot{\mathfrak{s}}(t) \in \mathrm{loc}(\mathfrak{h}) \cup \dot{\mathfrak{s}}(\mathbb{C})$.

For the induction step $\|\mathfrak{h}\| > 1$, let $t = \mathsf{root}(q_j^i(\mathbf{u}_j^i))$, for some $i \in [\![1 \,..\, n]\!]$ and some $j \in [\![1 \,..\, k_j]\!]$. If $n > 1$ or $m > n$ in Equation (12), we have $(\dot{\mathfrak{s}}, \mathfrak{h}') \models_{\mathfrak{C}_\mathcal{S}} \ast_{j=1}^{k_i} q_j^i(\mathbf{u}_j^i) \mathrel{-\!\!\bullet} p_i(\mathbf{t}_i)$, for some heap $\mathfrak{h}' \subset \mathfrak{h}$, such that $\|\mathfrak{h}'\| \geq 1$ and, by the inductive hypothesis, we obtain $\dot{\mathfrak{s}}(t) \in \mathrm{loc}(\mathfrak{h}') \cup \dot{\mathfrak{s}}(\mathbb{C}) \subseteq \mathrm{loc}(\mathfrak{h}) \cup \dot{\mathfrak{s}}(\mathbb{C})$. Otherwise, $m = n = 1$ and the argument is similar to the one used in the base case. ◀

▶ **Lemma 45.** *Let $\phi = \ast_{j=1}^{k} q_j(\mathbf{u}_j) \mathrel{-\!\!\bullet} p_i(\mathbf{t})$ be a core formula and let $(\dot{\mathfrak{s}}, \mathfrak{h})$ be an injective structure. If $\mathcal{S}$ is progressing and normalized, $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \phi$ and $x \in \mathbf{t} \setminus (\bigcup_{j=1}^{k} \mathbf{u}_j)$ then $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h})$.*

Proof: We reason by induction on $\|\mathfrak{h}\|$. If $\mathfrak{h} = \emptyset$ then by Lemma 43, we must have $k = 1$ and $\mathbf{u}_1 = \mathbf{t}$, thus $\mathbf{t} \setminus (\bigcup_{j=1}^{k} \mathbf{u}_j)$ is empty, which contradicts our hypothesis. Otherwise, by definition of the rules in $\mathfrak{C}_\mathcal{S}$, there exists a rule $p(\mathbf{x}) \Leftarrow_\mathcal{S} \exists \mathbf{z} \;\; \psi * \ast_{j=1}^{m} p_j(\mathbf{w}_j)$, an associate $\dot{\bar{\mathfrak{s}}}$ of $\dot{\mathfrak{s}}$ and a substitution $\sigma : \mathbf{z} \rightharpoonup \mathbf{x} \cup \bigcup_{j=1}^{m} \mathbf{y}_j$ such that $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi\sigma\theta * \ast_{j=1}^{m} \big(\gamma_j \mathrel{-\!\!\bullet} p_j(\sigma(\mathbf{w}_j))\big)\theta$, where $\ast_{j=1}^{m} \gamma_j = \ast_{j=1}^{k} q_j(\mathbf{y}_j)$ and $\theta = [\mathbf{t}/\mathbf{x}, \mathbf{u}_1/\mathbf{y}_1, \ldots, \mathbf{u}_m/\mathbf{y}_m]$. Since $\mathcal{S}$ is normalized, by Condition 2a in Definition 8, x occurs in all unfoldings of $p(\mathbf{t})$. Thus either x occurs in $\psi\theta$ (hence also in $\psi\sigma\theta$), or x occurs in $\mathbf{w}_j\theta$ (hence in $\mathbf{w}_j\sigma\theta$) for some $j \in [\![1 \,..\, m]\!]$. In the former case, necessarily $x \in \mathrm{loc}(\mathfrak{h})$, because ψ is a points-to atom, since $\mathcal{S}$ is progressing. In the latter case, we have $(\dot{\mathfrak{s}}, \mathfrak{h}') \models_{\mathfrak{C}_\mathcal{S}} \gamma_j \mathrel{-\!\!\bullet} p_j(\sigma(\mathbf{w}_j))\theta$, for some subheap $\mathfrak{h}'$ of $\mathfrak{h}$, with $\|\mathfrak{h}'\| < \|\mathfrak{h}\|$. Since $x \notin \bigcup_{j=1}^{k} \mathbf{u}_j$ by hypothesis and $\ast_{j=1}^{m} \gamma_j = \ast_{j=1}^{k} q_j(\mathbf{y}_j)$ we have $x \notin \mathsf{fv}(\gamma_j\theta)$, thus $x \in \mathbf{w}_j \setminus \mathsf{fv}(\gamma_j)\theta$. By the induction hypothesis, we deduce that $x \in \mathrm{loc}(\mathfrak{h}')$, hence $x \in \mathrm{loc}(\mathfrak{h})$. ◀

▶ **Proposition 46.** *Consider a quantifier-free symbolic heap φ and an injective substitution σ. If $\phi \in \mathcal{T}(\varphi)$ then $\phi\sigma \in \mathcal{T}(\varphi\sigma)$.*

The following lemmas relate a symbolic heap ϕ with the core formulæ $\psi \in \mathcal{T}(\phi)$, by considering separately the cases where ϕ is quantifier-free, or existentially quantified. In the latter case, we require moreover that the set of rules providing the interpretation of predicates be normalized.

▶ **Lemma 47.** *Given a quantifier-free symbolic heap $\phi \in \mathsf{SH}^\mathfrak{K}$, containing only predicate atoms that are contexts, an injective structure $(\dot{\mathfrak{s}}, \mathfrak{h})$ is a $\mathfrak{C}_\mathcal{S}$-model of ϕ iff $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$, for some $\psi \in \mathcal{T}(\phi)$.*

Proof: "⇒" By induction on the structure of ϕ. We consider the following cases:

- $\phi = \mathsf{emp}$, $\phi = t_0 \mapsto (t_1, \ldots, t_\mathfrak{K})$ and $\phi = \ast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$: in these cases, the only element in $\mathcal{T}(\phi)$ is ϕ itself and we have the result.
- $\phi = t_1 \doteq t_2$: since $(\dot{\mathfrak{s}}, \mathfrak{h}) \models t_1 \doteq t_2$, we have $\dot{\mathfrak{s}}(t_1) = \dot{\mathfrak{s}}(t_2)$ and $\mathfrak{h} = \emptyset$. Since $\dot{\mathfrak{s}}$ is injective, we obtain $t_1 = t_2$, $\mathcal{T}(\phi) = \{\mathsf{emp}\}$ and $(\dot{\mathfrak{s}}, \mathfrak{h}) \models \mathsf{emp}$, because $\mathfrak{h} = \emptyset$.
- $\phi = t_1 \neq t_2$: since $(\dot{\mathfrak{s}}, \mathfrak{h}) \models t_1 \neq t_2$, we have $\dot{\mathfrak{s}}(t_1) \neq \dot{\mathfrak{s}}(t_2)$ and $\mathfrak{h} = \emptyset$, therefore $t_1 \neq t_2$, $\mathcal{T}(t_1 \neq t_2) = \{\mathsf{emp}\}$ and $(\dot{\mathfrak{s}}, \mathfrak{h}) \models \mathsf{emp}$, because $\mathfrak{h} = \emptyset$.
- $\phi = \phi_1 * \phi_2$: since $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_\mathcal{S} \phi_1 * \phi_2$, there exist heaps $\mathfrak{h}_1$ and $\mathfrak{h}_2$, such that $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$ and $(\dot{\mathfrak{s}}, \mathfrak{h}_i) \models_\mathcal{S} \phi_i$, for $i = 1, 2$. By the inductive hypothesis, there exists $\psi_i \in \mathcal{T}(\phi_i)$ such that $(\dot{\mathfrak{s}}, \mathfrak{h}_i) \models_{\mathfrak{C}_\mathcal{S}} \psi_i$, for $i = 1, 2$. Then $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi_1 * \psi_2$, where $\psi_1 * \psi_2 \in \mathcal{T}(\phi_1 * \phi_2)$.

"⇐" By induction on the structure of ϕ, we consider only the equational atoms below, the proofs in the remaining cases are straightforward:

- $\phi = t_1 \doteq t_2$: since there exists $\psi \in \mathcal{T}(\phi)$ such that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_\mathcal{S} \psi$, necessarily $\mathcal{T}(\phi) = \{\mathsf{emp}\}$, which implies that $t_1 = t_2$. Since $(\dot{\mathfrak{s}}, \mathfrak{h}) \models \mathsf{emp}$, $\mathfrak{h} = \emptyset$ and $(\dot{\mathfrak{s}}, \mathfrak{h}) \models t_1 \doteq t_2$.
- $\phi = t_1 \neq t_2$: since there exists $\psi \in \mathcal{T}(\phi)$ such that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_\mathcal{S} \psi$, necessarily $\mathcal{T}(\phi) = \{\mathsf{emp}\}$, which implies that $t_1 \neq t_2$. Since $(\dot{\mathfrak{s}}, \mathfrak{h}) \models \mathsf{emp}$, $\mathfrak{h} = \emptyset$ and $(\dot{\mathfrak{s}}, \mathfrak{h}) \models t_1 \neq t_2$, by injectivity of $\dot{\mathfrak{s}}$. ◀

G Proof of Lemma 20 (Section 5)

"⇒" By induction on size(ϕ). We consider the following cases:

- $\phi = \mathsf{emp}$, $\phi = t_0 \mapsto (t_1, \ldots, t_\mathfrak{K})$, $\phi = t_1 \doteq t_2$, $\phi = t_1 \neq t_2$ and $\phi = \phi_1 * \phi_2$: the proof is the same as the one in Lemma 47.
- $\phi = p(\mathbf{t})$: in this case $\mathcal{T}(\phi) = \{\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})\}$ and the conclusion follows application of Lemma 42.
- $\phi = \exists x \,.\, \phi_1$: since $(\dot{s}, \mathfrak{h}) \models_\mathcal{S} \exists x \,.\, \phi_1$, there exists $\ell \in \mathbb{L}$ such that $(\dot{s}[x \leftarrow \ell], \mathfrak{h}) \models_\mathcal{S} \phi_1$ and we distinguish the following cases.
  - If $\ell \notin \dot{s}(\mathsf{fv}(\phi) \cup \mathbb{C})$, since ϕ is normalized, by Definition 8 (1a) x occurs in a points-to or in a predicate atom of ϕ_1. Since $\mathcal{S}$ is normalized, by Definition 8 (2a), we have that $\ell \in \mathrm{loc}(\mathfrak{h})$. Since $\mathrm{dom}(\dot{s}) = \mathsf{fv}(\phi) \cup \mathbb{C}$, the store $\dot{s}[x \leftarrow \ell]$ is necessarily injective, hence $(\dot{s}[x \leftarrow \ell], \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi_1$, for some $\psi_1 \in \mathcal{T}(\phi_1)$, by the inductive hypothesis and $(\dot{s}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \exists_\mathfrak{h} x \,.\, \psi_1$, by Lemma 41.
  - Otherwise, $\ell \in \dot{s}(\mathsf{fv}(\phi) \cup \mathbb{C})$ and let $t \in \mathsf{fv}(\phi) \cup \mathbb{C}$ be a term such that $\ell = \dot{s}(t)$. Then $(\dot{s}, \mathfrak{h}) \models_\mathcal{S} \phi_1[t/x]$ and $(\dot{s}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi_1$, for some $\psi_1 \in \mathcal{T}(\phi_1[t/x])$, by the inductive hypothesis.

"⇐" By induction on size(ϕ), considering the following cases:

- $\phi = \mathsf{emp}$, $\phi = t_0 \mapsto (t_1, \ldots, t_\mathfrak{K})$, $\phi = t_1 \doteq t_2$, $\phi = t_1 \neq t_2$ and $\phi = \phi_1 * \phi_2$: the proof is the same as the one in Lemma 47.
- $\phi = p(\mathbf{t})$: in this case $\psi = \mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$ is the only possibility and the conclusion follows by an application of Lemma 42.
- $\phi = \exists x \,.\, \phi_1$: by the definition of $\mathcal{T}(\phi)$, we distinguish the following cases:
  - If $(\dot{s}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \exists_\mathfrak{h} x \,.\, \psi_1$, for some $\psi_1 \in \mathcal{T}(\phi_1)$, then $(\dot{s}[x \leftarrow \ell], \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi_1$, for some $\ell \in \mathrm{loc}(\mathfrak{h}) \setminus \dot{s}((\mathsf{fv}(\psi_1) \setminus \{x\}) \cup \mathbb{C})$. By the definition of $\mathcal{T}(\phi_1)$, we have $\mathsf{fv}(\psi_1) \subseteq \mathsf{fv}(\phi_1)$ and suppose, for a contradiction, that there exists a variable $y \in \mathsf{fv}(\phi_1) \setminus \mathsf{fv}(\psi_1)$. Then y can only occur either in an equality atom $y \doteq y$ or in some disequality $y \neq t$, for some term $t \neq y$, and nowhere else. Both cases are impossible, because ϕ is normalized, thus by Condition (1b) of Definition 8, y necessarily occurs in a points-to or predicate atom. Hence, $\mathsf{fv}(\phi_1) = \mathsf{fv}(\psi_1)$ and consequently, we obtain $\ell \in \mathrm{loc}(\mathfrak{h}) \setminus \dot{s}((\mathsf{fv}(\phi_1) \setminus \{x\}) \cup \mathbb{C})$. Since $\mathrm{dom}(\dot{s}) = (\mathsf{fv}(\phi_1) \setminus \{x\}) \cup \mathbb{C}$, by the hypothesis of the Lemma, $\dot{s}[x \leftarrow \ell]$ is injective and, by the induction hypothesis, we obtain $(\dot{s}[x \leftarrow \ell], \mathfrak{h}) \models_\mathcal{S} \phi_1$, thus $(\dot{s}, \mathfrak{h}) \models_\mathcal{S} \phi$.
  - Otherwise $(\dot{s}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$, for some $\psi \in \mathcal{T}(\phi_1[t/x])$ and some $t \in \mathsf{fv}(\phi) \cup \mathbb{C}$. By the induction hypothesis, we have $(\dot{s}, \mathfrak{h}) \models_\mathcal{S} \phi_1[t/x]$, thus $(\dot{s}, \mathfrak{h}) \models_\mathcal{S} \exists x \,.\, \phi_1$. ◀

H Additional Material for Core Formulæ (Section 5)

▶ **Lemma 48.** *Given an injective structure* $(\dot{s}, \mathfrak{h})$ *and a context predicate atom* $\circledast_{i=1}^n q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$*, we have* $(\dot{s}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \circledast_{i=1}^n q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$ *iff* $(\dot{\bar{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \varphi$*, for some core unfolding* $\circledast_{i=1}^n q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_\mathcal{S}} \varphi$ *and some injective extension* $\bar{s}$ *of* $\dot{s}$*.*

Proof: We assume w.l.o.g. a total well-founded order $\preceq$ on the set of terms $\mathbb{T}$ and, for a set $T \subseteq \mathbb{T}$, we denote by $\min_\preceq T$ the minimal term from T with respect to this order. In the following, let $\theta \stackrel{\text{def}}{=} [\mathbf{t}/\mathbf{x}, \mathbf{u}_1/\mathbf{y}_1, \ldots, \mathbf{u}_n/\mathbf{y}_n]$.

"⇒" If $(\dot{s}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \circledast_{i=1}^n q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$ then there exists a rule $\circledast_{i=1}^n q_i(\mathbf{y}_i) \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_\mathcal{S}} \exists \mathbf{z} \,.\, \phi$, where ϕ is quantifier-free, such that $(\dot{s}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \exists \mathbf{z} \,.\, \phi\theta$. Let $\bar{s}$ be a (not necessarily injective) $\mathbf{z}$-associate of $\dot{s}$ such that $(\bar{s}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \phi\theta$. We define a substitution τ, such that $\mathrm{dom}(\tau) \stackrel{\text{def}}{=} \mathsf{trm}(\phi\theta) \subseteq \mathrm{dom}(\bar{s})$ and for each $x \in \mathrm{dom}(\tau)$:

- if $x \in \mathrm{dom}(\dot{s})$ then $\tau(x) \stackrel{\text{def}}{=} x$,
- else, if $x \notin \mathrm{dom}(\dot{s})$ and $\bar{s}(x) = \dot{s}(y)$, for some $y \in \mathrm{dom}(\dot{s})$, then $\tau(x) \stackrel{\text{def}}{=} \min_\preceq \{z \in \mathrm{dom}(\dot{s}) \mid \dot{s}(z) = \dot{s}(y)\}$,
- otherwise, if $x \notin \mathrm{dom}(\dot{s})$ and $\bar{s}(x) \neq \dot{s}(y)$, for all $y \in \mathrm{dom}(\dot{s})$, then $\tau(x) \stackrel{\text{def}}{=} \min_\preceq \{y \in \mathrm{dom}(\bar{s}) \mid \bar{s}(y) = \bar{s}(x)\}$.

Let $E \stackrel{\text{def}}{=} \{\{y \in \mathrm{dom}(\bar{\mathfrak{s}}) \mid \bar{\mathfrak{s}}(y) = \bar{\mathfrak{s}}(x)\} \,\big|\, x \in \mathrm{dom}(\bar{\mathfrak{s}})\}$; by construction, the sets in E are pairwise disjoint. Let $\dot{\bar{\mathfrak{s}}}$ be the restriction of $\bar{\mathfrak{s}}$ to the set $\mathrm{dom}(\dot{\mathfrak{s}}) \cup \{\min_{\preceq} K \mid K \in E,\ K \cap \mathrm{dom}(\dot{\mathfrak{s}}) = \emptyset\}$. Because $\dot{\mathfrak{s}}$ is injective, $\dot{\bar{\mathfrak{s}}}$ is easily shown to also be injective, thus it is an injective extension of $\dot{\mathfrak{s}}$. Moreover, because $(\bar{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi\theta$ and $\bar{\mathfrak{s}}$ agrees with $\dot{\bar{\mathfrak{s}}} \circ \tau$ on $\mathrm{dom}(\dot{\bar{\mathfrak{s}}})$, we deduce that $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi(\tau \circ \theta)$. We conclude by noticing that $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \varphi$, for some $\varphi \in \mathcal{T}(\phi(\tau \circ \theta))$, by an application of Lemma 47, because $\phi(\tau \circ \theta)$ is quantifier-free.

"$\Leftarrow$" If $\circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathcal{S}} \varphi$, by Definition 21, we have $\varphi \in \mathcal{T}(\phi\theta)$, for some rule $\circledast_{i=1}^{n} q_i(\mathbf{y}_i) \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{z}\ .\ \phi$, where ϕ is quantifier-free, and some substitution $\theta = [\mathbf{t}/\mathbf{x}, \mathbf{u}_1/\mathbf{y}_1, \ldots, \mathbf{u}_n/\mathbf{y}_i] \cup \zeta$, where $\zeta \subseteq \{(z,t) \mid z \in \mathbf{z},\ t \in \mathbf{t} \cup \bigcup_{i=1}^{n} \mathbf{u}_i\}$. Since $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \varphi$ and $\phi\theta$ is quantifier-free, by Lemma 47, we obtain $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi\theta$, hence $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} (\exists \mathbf{z}\ .\ \phi)\theta$ and $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$ follows. ◀

▶ **Lemma 49.** *Given a bijective structure $(\dot{\mathfrak{s}}, \mathfrak{h})$ and a context predicate atom $\circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$, we have $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$ if and only if $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \varphi$, for some core unfolding $\circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} \varphi$.*

Proof: "$\Rightarrow$" Let $\dot{\mathfrak{s}}'$ be the restriction of $\dot{\mathfrak{s}}$ to $\mathbf{t} \cup \bigcup_{i=1}^{n} \mathbf{u}_i$. Clearly, we have $(\dot{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$. By Lemma 48, there exists a core unfolding $\circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} \phi$ and an injective extension $\dot{\bar{\mathfrak{s}}}$ of $\dot{\mathfrak{s}}'$, such that $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi$. Let τ be the substitution defined by $\tau(t) = u$ if and only if $\dot{\bar{\mathfrak{s}}}(t) = \dot{\mathfrak{s}}(u)$, for all $t \in \mathsf{trm}(\phi)$. Note that, since $\dot{\mathfrak{s}}$ is bijective, for each $t \in \mathrm{dom}(\dot{\bar{\mathfrak{s}}})$, there exists a unique $u \in \mathbb{T}$, such that $\dot{\bar{\mathfrak{s}}}(t) = \dot{\mathfrak{s}}(u)$, hence τ is well-defined. Furthermore, since $\dot{\bar{\mathfrak{s}}}$ is injective, τ is also injective. We have $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi\tau$ and we are left with proving that $\circledast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} \phi\tau$ is a core unfolding. By Proposition 46 we have $\phi\tau \in \mathcal{T}(\varphi\sigma\tau)$, hence the result. "$\Leftarrow$" This is a consequence of Lemma 48, using the fact that $\dot{\mathfrak{s}}$ is an injective extension of itself. ◀

The following property of core formulæ leads to a necessary and sufficient condition for their satisfiability (Lemma 52). The idea is that the particular identity of locations outside of the heap, assigned by the $\forall_{\neg\mathfrak{h}}$ quantifier, is not important when considering a model of a core formula.

▶ **Definition 50.** *For a set of locations $L \subseteq \mathbb{L}$, we define $\dot{\mathfrak{s}} \approx_L \dot{\mathfrak{s}}'$ if and only if $\mathrm{dom}(\dot{\mathfrak{s}}) = \mathrm{dom}(\dot{\mathfrak{s}}')$ and, for each term $t \in \mathrm{dom}(\dot{\mathfrak{s}})$, if $\{\dot{\mathfrak{s}}(t), \dot{\mathfrak{s}}'(t)\} \cap L \neq \emptyset$ then $\dot{\mathfrak{s}}(t) = \dot{\mathfrak{s}}'(t)$.*

It is easy to check that $\approx_L$ is an equivalence relation, for each set $L \subseteq \mathbb{L}$.

▶ **Lemma 51.** *Let $\dot{\mathfrak{s}}$ and $\dot{\mathfrak{s}}'$ be two injective stores and $\mathfrak{h}$ be a heap, such that $\dot{\mathfrak{s}} \approx_{\mathrm{loc}(\mathfrak{h})} \dot{\mathfrak{s}}'$. If $\mathcal{S}$ is progressing, then for every core formula φ, we have $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \varphi$ if and only if $(\dot{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \varphi$.*

Proof: We assume that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \varphi$ and show that $(\dot{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \varphi$; the proof in the other direction is identical since $\approx_{\mathrm{loc}(\mathfrak{h})}$ is symmetric. The proof is carried out by nested induction on $\|\mathfrak{h}\|$ and $\mathrm{size}(\varphi)$. We assume, w.l.o.g., that $\mathrm{dom}(\dot{\mathfrak{s}}) = \mathrm{dom}(\dot{\mathfrak{s}}') = \mathsf{fv}(\varphi) \cup \mathbb{C}$. This is without loss of generality since the truth value of φ in $(\dot{\mathfrak{s}}, \mathfrak{h})$ and $(\dot{\mathfrak{s}}', \mathfrak{h})$ depends only on the restriction of $\dot{\mathfrak{s}}$ (resp. $\dot{\mathfrak{s}}'$) to $\mathsf{fv}(\varphi) \cup \mathbb{C}$.

For the base case assume that $\|\mathfrak{h}\| = 0$. By hypothesis, $\varphi = \exists_{\mathfrak{h}} \mathbf{x} \forall_{\neg\mathfrak{h}} \mathbf{y}\ .\ \circledast_{i=1}^{n} \left(\circledast_{j=1}^{k_i} q_j^i(\mathbf{u}_j^i) \mathrel{-\!\!\bullet} p_i(\mathbf{t}_i) \right) * \circledast_{i=n+1}^{m} x_i \mapsto (t_1^i, \ldots, t_{\mathfrak{K}}^i)$ and since $\mathfrak{h} = \emptyset$, necessarily, $\mathbf{x} = \emptyset$ and $m = 0$. Let $\dot{\mathfrak{s}}_1$ be an injective $\mathbf{y}$-associate of $\dot{\mathfrak{s}}$, where for all $y \in \mathbf{y}$, we have $\dot{\mathfrak{s}}_1(y) \in \mathbb{L} \setminus [\dot{\mathfrak{s}}((\mathsf{fv}(\varphi) \cup \mathbf{y}) \cup \mathbb{C})]$. Note that such a store exists because $\mathbb{L}$ is infinite, wherease $\mathrm{dom}(\dot{\mathfrak{s}})$ and $\mathbf{y}$ are both finite. By Lemma 41 we have $(\dot{\mathfrak{s}}_1, \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \circledast_{i=1}^{n} \left(\circledast_{j=1}^{k_i} q_j^i(\mathbf{u}_j^i) \mathrel{-\!\!\bullet} p_i(\mathbf{t}_i) \right)$. Thus for $i \in [\![1 \,..\, n]\!]$ we have $(\dot{\mathfrak{s}}_1, \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \circledast_{j=1}^{k_i} q_j^i(\mathbf{u}_j^i) \mathrel{-\!\!\bullet} p_i(\mathbf{t}_i)$, and by Lemma 43, we deduce that $k_i = 1$, $q_1^i = p_i$ and $\dot{\mathfrak{s}}_1(\mathbf{u}_1^i) = \dot{\mathfrak{s}}_1(\mathbf{t}_i)$. Since $\dot{\mathfrak{s}}_1$ is injective, we deduce that $\mathbf{u}_1^i = \mathbf{t}_i$, but this is impossible because by hypothesis, the roots of a core formula are unique. Hence $(\dot{\mathfrak{s}}, \mathfrak{h}) \not\models_{\mathfrak{C}_{\mathcal{S}}} \varphi$ and the implication holds.

For the induction step assume that $\|\mathfrak{h}\| > 0$, we consider the following cases:

- $\varphi = \mathsf{emp}$: since $\|\mathfrak{h}\| > 0$, we cannot have $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \mathsf{emp}$.

- $\varphi = t_0 \mapsto (t_1, \ldots, t_\Re)$: in this case $\mathfrak{h} = \{(\dot{\mathfrak{s}}(t_0), (\dot{\mathfrak{s}}(t_1), \ldots, \dot{\mathfrak{s}}(t_\Re)))\}$ and since $\dot{\mathfrak{s}}(t_0), \dot{\mathfrak{s}}(t_1), \ldots, \dot{\mathfrak{s}}(t_\Re) \in \mathrm{loc}(\mathfrak{h})$ and $\dot{\mathfrak{s}} \approx_{\mathrm{loc}(\mathfrak{h})} \dot{\mathfrak{s}}'$, we also have $\mathfrak{h} = \{(\dot{\mathfrak{s}}'(t_0), (\dot{\mathfrak{s}}'(t_1), \ldots, \dot{\mathfrak{s}}'(t_\Re)))\}$, thus $(\dot{\mathfrak{s}}', \mathfrak{h}) \models t_0 \mapsto (t_1, \ldots, t_\Re)$.
- $\varphi = \mathbin{\ast}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$: since $\|\mathfrak{h}\| > 0$, φ cannot be $p(\mathbf{t}) \mathrel{-\!\!\bullet} p(\mathbf{t})$. Thus the first unfolding step is an instance of a rule obtained from II. By Lemma 48, there exists an injective extension $\dot{\bar{\mathfrak{s}}}$ of $\dot{\mathfrak{s}}$ such that $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$ where $\varphi \rightsquigarrow_{\mathfrak{C}_\mathcal{S}} \psi$, and because $\mathcal{S}$ is progressing, ψ is of the form $t_0 \mapsto (t_1, \ldots, t_\Re) * \psi'$. Since the truth value of ψ in $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h})$ depends only on the restriction of $\dot{\bar{\mathfrak{s}}}$ to $\mathsf{fv}(\varphi) \cup \mathbb{C}$, we assume, w.l.o.g., that $\mathrm{dom}(\dot{\bar{\mathfrak{s}}})$ is finite. The heap $\mathfrak{h}$ can thus be decomposed into $\mathfrak{h}_0 \uplus \mathfrak{h}'$, where $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}_0) \models_{\mathfrak{C}_\mathcal{S}} t_0 \mapsto (t_1, \ldots, t_\Re)$ and $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}') \models_{\mathfrak{C}_\mathcal{S}} \psi'$. Consider the store $\mathfrak{s}_1 \stackrel{\text{def}}{=} \{(x, \dot{\bar{\mathfrak{s}}}(x)) \mid x \in \mathrm{dom}(\dot{\bar{\mathfrak{s}}}) \setminus \mathrm{dom}(\dot{\mathfrak{s}}) \wedge \dot{\bar{\mathfrak{s}}}(x) \in \mathrm{loc}(\mathfrak{h})\}$ and let $\dot{\mathfrak{s}}_1 \stackrel{\text{def}}{=} \dot{\mathfrak{s}}' \cup \mathfrak{s}_1$. Since $\mathrm{dom}(\dot{\mathfrak{s}}) = \mathrm{dom}(\dot{\mathfrak{s}}')$ by hypothesis, $\dot{\mathfrak{s}}_1$ is well-defined. It is also injective because $\dot{\mathfrak{s}}'$ and $\dot{\bar{\mathfrak{s}}}$ are both injective, and if $\dot{\mathfrak{s}}_1(x) = \dot{\mathfrak{s}}_1(y)$, where $x \in \mathrm{dom}(\dot{\mathfrak{s}}')$ and $y \in \mathrm{dom}(\mathfrak{s}_1)$, then $\dot{\mathfrak{s}}_1(y) = \dot{\bar{\mathfrak{s}}}(y) \in \mathrm{loc}(\mathfrak{h})$, hence we also have $\dot{\mathfrak{s}}_1(x) = \dot{\mathfrak{s}}'(x) \in \mathrm{loc}(\mathfrak{h})$. By hypothesis $\dot{\mathfrak{s}} \approx_{\mathrm{loc}(\mathfrak{h})} \dot{\mathfrak{s}}'$, hence $\dot{\mathfrak{s}}'(x) = \dot{\mathfrak{s}}(x) = \dot{\bar{\mathfrak{s}}}(x)$, so that $\dot{\bar{\mathfrak{s}}}(x) = \dot{\bar{\mathfrak{s}}}(y)$. Since $\dot{\bar{\mathfrak{s}}}$ is injective, we deduce that $x = y$. Now let $\dot{\mathfrak{s}}_2$ be an injection from $\mathrm{dom}(\dot{\bar{\mathfrak{s}}}) \setminus \mathrm{dom}(\dot{\mathfrak{s}}_1)$ onto $\mathbb{L} \setminus \Big(\mathrm{rng}(\dot{\bar{\mathfrak{s}}}) \cup \mathrm{rng}(\dot{\mathfrak{s}}') \cup \mathrm{loc}(\mathfrak{h})\Big)$. Note that such an extension necessarily exists since $\mathrm{dom}(\dot{\bar{\mathfrak{s}}})$, $\mathrm{dom}(\dot{\mathfrak{s}}')$ and $\mathrm{loc}(\mathfrak{h})$ are all finite whereas $\mathbb{L}$ is infinite. Let $\dot{\bar{\mathfrak{s}}}' \stackrel{\text{def}}{=} \dot{\mathfrak{s}}_1 \cup \dot{\mathfrak{s}}_2$, it is straightforward to verify that $\dot{\bar{\mathfrak{s}}}'$ is injective and that $\dot{\bar{\mathfrak{s}}} \approx_{\mathrm{loc}(\mathfrak{h})} \dot{\bar{\mathfrak{s}}}'$. By the inductive hypothesis we have $(\dot{\bar{\mathfrak{s}}}', \mathfrak{h}_0) \models_{\mathfrak{C}_\mathcal{S}} t_0 \mapsto (t_1, \ldots, t_\Re)$ and $(\dot{\bar{\mathfrak{s}}}', \mathfrak{h}') \models_{\mathfrak{C}_\mathcal{S}} \psi'$, and by Lemma 48 we deduce that $(\dot{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \mathbin{\ast}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$.
- $\varphi = \exists_\mathsf{h} x \,.\, \psi$: by Lemma 41, there exists an x-associate $\bar{\mathfrak{s}}$ of $\dot{\mathfrak{s}}$, such that $\bar{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}) \setminus \dot{\mathfrak{s}}((\mathsf{fv}(\psi) \setminus \{x\}) \cup \mathbb{C})$ and $(\bar{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$. We distinguish two cases.
  - If $\bar{\mathfrak{s}}(x) = \dot{\mathfrak{s}}(y)$ for some $y \in \mathrm{dom}(\dot{\mathfrak{s}})$ then $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi[y/x]$ and, by the induction hypothesis, we have $(\dot{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi[y/x]$. Since $\dot{\mathfrak{s}} \approx_{\mathrm{loc}(\mathfrak{h})} \dot{\mathfrak{s}}'$ and $\dot{\mathfrak{s}}(y) \in \mathrm{loc}(\mathfrak{h})$, we have $\dot{\mathfrak{s}}(y) = \dot{\mathfrak{s}}'(y)$. Furthermore, since $\bar{\mathfrak{s}}(x) \notin \dot{\mathfrak{s}}((\mathsf{fv}(\psi) \setminus \{x\}) \cup \mathbb{C})$, necessarily $y \notin (\mathsf{fv}(\psi) \setminus \{x\}) \cup \mathbb{C}$ and, because $\dot{\mathfrak{s}}'$ is injective, $\dot{\mathfrak{s}}'(y) \notin \dot{\mathfrak{s}}'((\mathsf{fv}(\psi) \setminus \{x\}) \cup \mathbb{C})$. Since $\dot{\mathfrak{s}}'(y) = \bar{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h})$ and $(\dot{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi[y/x]$, we deduce that $(\dot{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \exists_\mathsf{h} x \,.\, \psi$.
  - Otherwise we have $\bar{\mathfrak{s}}(x) \neq \dot{\mathfrak{s}}(y)$ for all $y \in \mathrm{dom}(\dot{\mathfrak{s}})$ and $\bar{\mathfrak{s}}$ is therefore injective. Let $\bar{\mathfrak{s}}' \stackrel{\text{def}}{=} \dot{\mathfrak{s}}'[x \leftarrow \bar{\mathfrak{s}}(x)]$. Suppose that $\bar{\mathfrak{s}}(x) = \dot{\mathfrak{s}}'(y)$, for some $y \in \mathrm{dom}(\dot{\mathfrak{s}}')$. Since $\dot{\mathfrak{s}} \approx_{\mathrm{loc}(\mathfrak{h})} \dot{\mathfrak{s}}'$ we have $\mathrm{dom}(\dot{\mathfrak{s}}') = \mathrm{dom}(\dot{\mathfrak{s}})$, hence $y \in \mathrm{dom}(\dot{\mathfrak{s}})$ and, since $\dot{\mathfrak{s}}(y) \in \mathrm{loc}(\mathfrak{h})$, we obtain $\dot{\mathfrak{s}}(y) = \dot{\mathfrak{s}}'(y) = \bar{\mathfrak{s}}(x)$, in contradiction with the assumption of this case. Thus $\bar{\mathfrak{s}}'$ is injective and, using the fact that $\bar{\mathfrak{s}} \approx_{\mathrm{loc}(\mathfrak{h})} \bar{\mathfrak{s}}'$, we deduce that $(\bar{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$ by the induction hypothesis. Since $\bar{\mathfrak{s}}'(x) = \bar{\mathfrak{s}}(x) \notin \mathrm{dom}(\dot{\mathfrak{s}}) = \mathrm{dom}(\dot{\mathfrak{s}}')$, we have $\bar{\mathfrak{s}}'(x) \notin \dot{\mathfrak{s}}'((\mathsf{fv}(\psi) \setminus \{x\}) \cup \mathbb{C})$. Moreover, $\bar{\mathfrak{s}}'(x) = \bar{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h})$, thus $(\dot{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \exists_\mathsf{h} x \,.\, \psi$ by Lemma 41.
- $\forall_{\neg\mathsf{h}} x \,.\, \psi$: By Lemma 41, $(\dot{\mathfrak{s}}, \mathfrak{h}) \models \forall_{\neg\mathsf{h}} x \,.\, \psi$ iff $(\dot{\mathfrak{s}}[x \leftarrow \ell] \models \psi$ holds for all locations $\ell \in \mathbb{L}$ such that $\ell \notin \mathrm{loc}(\mathfrak{h}) \cup \dot{\mathfrak{s}}(\mathsf{fv}(\forall_{\neg\mathsf{h}} x \,.\, \psi))$. Let $\ell \in \mathbb{L} \setminus [\mathrm{loc}(\mathfrak{h}) \cup \mathrm{rng}(\dot{\mathfrak{s}})]$ be an arbitrary location. Since $\mathbb{L}$ is infinite and $\mathrm{loc}(\mathfrak{h}) \cup \mathrm{rng}(\dot{\mathfrak{s}})$ is finite, such a location exists. By definition of $\forall_{\neg\mathsf{h}}$, we have $(\dot{\bar{\mathfrak{s}}}[x \leftarrow \ell], \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$. Now let $\ell' \in \mathbb{L} \setminus [\mathrm{loc}(\mathfrak{h}) \cup \mathrm{rng}(\dot{\mathfrak{s}}')]$ be an arbitrary location. Clearly $\dot{\mathfrak{s}}[x \leftarrow \ell]$ and $\dot{\mathfrak{s}}'[x \leftarrow \ell']$ are injective stores and $\dot{\mathfrak{s}}[x \leftarrow \ell] \approx_{\mathrm{loc}(\mathfrak{h})} \dot{\mathfrak{s}}'[x \leftarrow \ell']$, since $\ell, \ell' \notin \mathrm{loc}(\mathfrak{h})$. By the induction hypothesis, we have $(\dot{\mathfrak{s}}'[x \leftarrow \ell'], \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$ and, since the choice of $\ell' \in \mathbb{L} \setminus [\mathrm{rng}(\dot{\mathfrak{s}}') \cup \mathrm{loc}(\mathfrak{h})] = \mathbb{L} \setminus [\dot{\mathfrak{s}}'(\mathsf{fv}(\varphi) \cup \mathbb{C}) \cup \mathrm{loc}(\mathfrak{h})]$ was arbitrary, $(\dot{\mathfrak{s}}', \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \forall_{\neg\mathsf{h}} x \,.\, \psi$, by definition of $\forall_{\neg\mathsf{h}}$. ◀

The following lemma gives an alternative condition for the satisfiability of core formulæ. Intuitively, it is sufficient to instantiate the bounded universal quantifiers with arbitrary locations that are not in the image of the store, nor in the range of the heap.

▶ **Lemma 52.** *Given a core formula $\varphi = \exists_\mathsf{h} \mathbf{x} \forall_{\neg\mathsf{h}} \mathbf{y} \,.\, \psi$, where ψ is quantifier-free, and an injective structure $(\dot{\mathfrak{s}}, \mathfrak{h})$, such that $\mathrm{dom}(\dot{\mathfrak{s}}) = \mathsf{fv}(\varphi) \cup \mathbb{C}$, we have $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \varphi$ if and only if $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$, for some injective $(\mathbf{x} \cup \mathbf{y})$-associate $\dot{\bar{\mathfrak{s}}}$ of $\dot{\mathfrak{s}}$, such that $\dot{\bar{\mathfrak{s}}}(\mathbf{x}) \subseteq \mathrm{loc}(\mathfrak{h})$ and $\dot{\bar{\mathfrak{s}}}(\mathbf{y}) \cap \mathrm{loc}(\mathfrak{h}) = \emptyset$.*

Proof: "⇒" Since $\mathbb{L}$ is infinite and $\mathrm{dom}(\dot{\mathfrak{s}}) \cup \mathrm{loc}(\mathfrak{h})$ is finite, there exists an injective $(\mathbf{x} \cup \mathbf{y})$-associate $\dot{\bar{\mathfrak{s}}}$ of $\dot{\mathfrak{s}}$, such that $\dot{\bar{\mathfrak{s}}}(\mathbf{x}) \subseteq \mathrm{loc}(\mathfrak{h})$, $\dot{\bar{\mathfrak{s}}}(\mathbf{y}) \cap \mathrm{loc}(\mathfrak{h}) = \emptyset$ and $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$, by the semantics of the bounded quantifiers $\exists_\mathsf{h}$ and $\forall_{\neg\mathsf{h}}$ (see Lemma 41).

"⇐" Let $\mathbf{x} = \{x_1, \ldots, x_n\}$, $\mathbf{y} = \{y_1, \ldots, y_m\}$ and let $\ell_1, \ldots, \ell_n \in \mathrm{loc}(\mathfrak{h}) \setminus \dot{\mathfrak{s}}((\mathsf{fv}(\psi) \setminus (\mathbf{x} \cup \mathbf{y})) \cup \mathbb{C})$ and $\ell_{n+1}, \ldots, \ell_{n+m} \in \mathbb{L} \setminus (\mathrm{loc}(\mathfrak{h}) \cup \dot{\mathfrak{s}}((\mathsf{fv}(\psi) \setminus \mathbf{y}) \cup \mathbb{C}))$ be arbitrary locations, since $\mathbb{L}$ is infinite and $\mathsf{fv}(\psi) \cup \mathbb{C} \cup \mathrm{loc}(\mathfrak{h})$ is finite, such locations necessarily exist. Let $\dot{\mathfrak{s}} = \dot{\mathfrak{s}}[x_1 \leftarrow \ell_1, \ldots, x_n \leftarrow \ell_n]$. Then $\dot{\mathfrak{s}}[y_1 \leftarrow \ell_{n+1}, \ldots, y_m \leftarrow \ell_{n+m}] \approx_{\mathrm{loc}(\mathfrak{h})} \dot{\mathfrak{s}}$, thus $(\dot{\mathfrak{s}}[y_1 \leftarrow \ell_{n+1}, \ldots, y_m \leftarrow \ell_{n+m}], \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \psi$, by Lemma 51. Since the choice of $\ell_{n+1}, \ldots, \ell_{n+m}$ is arbitrary, we deduce that $(\dot{\mathfrak{s}}[y_1 \leftarrow \ell_{n+1}, \ldots, y_m \leftarrow \ell_{n+m}], \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \forall_{\neg \mathsf{h}} y \,.\, \psi$ and that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \exists_{\mathsf{h}} x \forall_{\neg \mathsf{h}} y \,.\, \psi$. ◀

I Proof of Lemma 25 (Section 5)

"⇒" Let $\phi \vdash_\mathcal{P} \psi_1, \ldots, \psi_n$ be a sequent and $\varphi \in \mathcal{T}(\phi)$ be a core formula. Since ϕ is quantifier-free and $\mathsf{fv}(\phi) = \emptyset$ (Definition 3), we deduce that φ is quantifier-free and $\mathrm{roots}(\varphi) \subseteq \mathsf{trm}(\phi) \subseteq \mathbb{C}$, hence $\varphi \in \mathsf{Core}(\mathcal{P})$, by Definition 22. If there is no set of core formulæ $F \in 2^{\mathsf{Core}(\mathcal{P})}$ such that $(\varphi, F) \in \mathcal{F}$, then there is nothing to prove. Otherwise, let $F \in 2^{\mathsf{Core}(\mathcal{P})}$ be a set of core formulæ, such that $(\varphi, F) \in \mathcal{F}$. By Definition 24, there exists an injective normal $\mathfrak{C}_\mathcal{S}$-model $(\dot{\mathfrak{s}}, \mathfrak{h})$ of φ, such that $F = C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h})$. Since $\mathcal{P}$ is valid, $\phi \models_\mathcal{S} \bigvee_{i=1}^n \psi_i$, hence there exists $i \in [\![1 \,..\, n]\!]$, such that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_\mathcal{S} \psi_i$. Since $\mathrm{dom}(\dot{\mathfrak{s}}) = \mathbb{C} = \mathsf{fv}(\psi_i) \cup \mathbb{C}$, by Lemma 20, we obtain $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \zeta$, for some $\zeta \in \mathcal{T}(\psi_i)$. Since $\mathsf{fv}(\zeta) \subseteq \mathsf{fv}(\psi_i) = \emptyset$, we also have that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_\mathcal{S} \zeta$. We show that $\zeta \in \mathsf{Core}(\mathcal{P})$. First, all predicate atoms in ζ are of the form $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$, and if ζ contains two distinct occurrences of atoms $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$ and $\mathsf{emp} \mathrel{-\!\!\bullet} q(\mathbf{s})$ with $\mathrm{roots}(p(\mathbf{t})) = \mathrm{roots}(q(\mathbf{s}))$ then ζ cannot be satisfiable, because the same location cannot be allocated in two disjoint parts of the heap. Second, since $\mathcal{P}$ is normalized, all existential variables must occur in a predicate or points-to atom. Thus all the conditions of Definition 19 are satisfied. Finally, since $\|\mathcal{V}^2_\mathcal{P}\| = \mathrm{width}(\mathcal{P}) \geq \mathrm{size}(\psi_i)$, we may assume up to an α-renaming that all the bound variables in ψ_i are in $\mathcal{V}^2_\mathcal{P}$, hence the same holds for ζ. Since any predicate atom that occurs in a core formula in $\mathcal{T}(\psi_i)$ is of the form $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$, we have $\mathrm{roots}_{\mathsf{lhs}}(\psi_i \sigma) = \emptyset$. By Definition 23, we have $\zeta \in C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h}) = F$, thus $F \cap \mathcal{T}(\psi_i) \neq \emptyset$.

"⇐" Let $\phi \vdash_\mathcal{P} \psi_1, \ldots, \psi_n$ be a sequent. Let $(\dot{\mathfrak{s}}, \mathfrak{h})$ be an $\mathcal{S}$-model of ϕ. Since $\mathsf{fv}(\phi) = \mathsf{fv}(\psi_1) = \cdots = \mathsf{fv}(\psi_n) = \emptyset$, we may assume, w.l.o.g., that $\mathrm{dom}(\mathfrak{s}) = \mathbb{C}$, and that $\dot{\mathfrak{s}}$ is injective (by Assumption 1 all constants are mapped to pairwise distinct locations). It is sufficient to prove that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_\mathcal{S} \psi_i$, for some $i \in [\![1 \,..\, n]\!]$, because in this case, we also have $(\mathfrak{s}, \mathfrak{h}) \models_\mathcal{S} \psi_i$. By Lemma 17, it is sufficient to show that any injective normal $\mathcal{S}$-model of ϕ is an $\mathcal{S}$-model of ψ_i, for some $i \in [\![1 \,..\, n]\!]$, so let us assume that $(\dot{\mathfrak{s}}, \mathfrak{h})$ is also a normal $\mathcal{S}$-model of ϕ. Since $\mathsf{fv}(\phi) = \emptyset$, by Lemma 47, we have $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \varphi$, for some $\varphi \in \mathcal{T}(\phi)$. By Definition 24, we have $(\varphi, C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h})) \in \mathcal{F}$, hence $C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h}) \cap \mathcal{T}(\psi_i) \neq \emptyset$, for some $i \in [\![1 \,..\, n]\!]$. Then there exists a core formula $\zeta \in \mathcal{T}(\psi_i)$, such that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \zeta$, by Definition 23 and, since $\mathrm{dom}(\dot{\mathfrak{s}}) = \mathbb{C} = \mathsf{fv}(\psi_i) \cup \mathbb{C}$, by Lemma 20, we obtain $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_\mathcal{S} \psi_i$. Since the choice of $(\dot{\mathfrak{s}}, \mathfrak{h})$ is arbitrary, each injective normal $\mathcal{S}$-model of $\phi\sigma$ is a model of $\psi_i \sigma$, for some $i \in [\![1 \,..\, n]\!]$. ◀

J Additional Material for the Construction of Profiles (Section 6)

▶ **Lemma 53.** *If $\mathcal{S}$ is progressing, then for all terms $t_0, \ldots, t_\aleph \in \mathcal{V}^1_\mathcal{P} \cup \mathbb{C}$ and all sets of core formulæ $F \in 2^{\mathsf{Core}(\mathcal{P})}$, we have $(t_0 \mapsto (t_1, \ldots, t_\aleph), F) \in \mathcal{F}_\mathcal{P}$ if and only if $F = C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h})$, for some injective $\mathcal{S}$-model $(\dot{\mathfrak{s}}, \mathfrak{h})$ of $t_0 \mapsto (t_1, \ldots, t_\aleph)$, such that* $\mathrm{dom}(\dot{\mathfrak{s}}) = \{t_0, \ldots, t_\aleph\} \cup \mathbb{C}$.

Proof: Let $(\dot{\mathfrak{s}}, \mathfrak{h})$ be an arbitrary injective model of $t_0 \mapsto (t_1, \ldots, t_\aleph)$ where $\mathrm{dom}(\dot{\mathfrak{s}}) = \{t_0, \ldots, t_\aleph\} \cup \mathbb{C}$ and $\mathfrak{h} = \{(\dot{\mathfrak{s}}(t_0), (\dot{\mathfrak{s}}(t_1), \ldots, \dot{\mathfrak{s}}(t_\aleph)))\}$. We show $F = C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h})$ below, where F is defined by (1):

"⊆" Let $\phi \in F$ and consider the following cases:

- If $\phi = t_0 \mapsto (t_1, \ldots, t_\aleph)$ then $(\dot{\mathfrak{s}}, \mathfrak{h}) \models t_0 \mapsto (t_1, \ldots, t_\aleph)$ and $\mathrm{roots}_{\mathsf{lhs}}(\phi) = \emptyset$, thus $\phi \in C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h})$ (see Definition 23).
- Otherwise, $\phi = \forall_{\neg \mathsf{h}} \mathbf{z} \,.\, \mathbin{\ast}_{i=1}^n q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$, where $\mathbf{z} = \left(\bigcup_{i=1}^n \mathbf{u}_i \cup \mathbf{t}\right) \setminus (\{t_0, \ldots, t_\aleph\} \cup \mathbb{C})$ and $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_\mathcal{S}} t_0 \mapsto (t_1, \ldots, t_\aleph) \mathbin{\ast} \mathbin{\ast}_{i=1}^n \mathsf{emp} \mathrel{-\!\!\bullet} q_i(\mathbf{u}_i)$. Note that by the progressivity condition, we have

$t_0 = \mathsf{root}(p(\mathbf{t}))$. By Definition 21, there exists a rule:

$$\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{v} \,.\, \psi * \mathop{\Large *}_{i=1}^{n} (\mathsf{emp} \mathrel{-\!\!\bullet} q_i(\mathbf{y}_i)) \;\; (\dagger)$$

such that $t_0 \mapsto (t_1, \ldots, t_{\Re}) \in \mathcal{T}(\psi\sigma)$ and σ is an extension of $[\mathbf{t}/\mathbf{x}, \mathbf{u}_1/\mathbf{y}_1, \ldots, \mathbf{y}_n/\mathbf{u}_n]$ with pairs (z,t), where $z \in \mathbf{v}$ and $t \in \mathbf{t} \cup \bigcup_{i=1}^{n} \mathbf{u}_i$. By (II), the rule $(\dagger)$ occurs because of the existence of a rule

$$p(\mathbf{x}) \Leftarrow_{\mathcal{S}} \exists \mathbf{w} \,.\, \varphi * \mathop{\Large *}_{i=1}^{n} q_i(\mathbf{z}_i) \;\; (\dagger\dagger)$$

and a substitution $\tau : \mathbf{w} \rightharpoonup \mathbf{x}$, such that $\psi = \varphi\tau$, $\mathbf{v} = \mathbf{w} \setminus \mathrm{dom}(\tau)$ and $\mathbf{y}_i = \tau(\mathbf{z}_i)$, for all $i \in [\![1 \,..\, n]\!]$. Applying τ to $(\dagger\dagger)$, by (II), we obtain the rule:

$$\mathop{\Large *}_{i=1}^{n} q_i(\mathbf{y}_i) \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{v} \,.\, \psi * \mathop{\Large *}_{i=1}^{n} (q_i(\mathbf{y}_i) \mathrel{-\!\!\bullet} q_i(\mathbf{y}_i)) \;\; (\ddagger)$$

Let $\dot{\bar{\mathfrak{s}}}$ be an injective $\mathbf{v}$-associate of $\dot{\mathfrak{s}}$. Such an associate necessarily exists, for instance if $\dot{\bar{\mathfrak{s}}}$ maps $\mathbf{v}$ into pairwise distinct locations, that are further distinct from $\mathrm{rng}(\dot{\mathfrak{s}})$; since $\mathbb{L}$ is infinite and $\mathrm{dom}(\dot{\mathfrak{s}})$ is assumed to be finite, such locations always exist. By α-renaming if necessary, we can assume that $\mathbf{v} \cap \{t_0, \ldots, t_{\Re}\} = \emptyset$, thus $\dot{\mathfrak{s}}$ and $\dot{\bar{\mathfrak{s}}}$ agree on $\{t_0, \ldots, t_{\Re}\}$ and we obtain $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models t_0 \mapsto (t_1, \ldots, t_{\Re})$. Since $t_0 \mapsto (t_1, \ldots, t_{\Re}) \in \mathcal{T}(\psi\sigma)$, by Lemma 47, we have $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models \psi\sigma$. By Lemma 43, we have $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \psi\sigma * \mathop{\Large *}_{i=1}^{n} (q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} q_i(\mathbf{u}_i))$ and, by rule $(\ddagger)$ we obtain $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \mathop{\Large *}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$. There remains to prove that $\dot{\bar{\mathfrak{s}}} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}, \mathfrak{h}, \phi)$. Since there are no existentially quantified variables in ϕ, it suffices to show that $\dot{\bar{\mathfrak{s}}}(\mathbf{z}) \cap \mathrm{loc}(\mathfrak{h}) = \dot{\bar{\mathfrak{s}}}(\mathbf{z}) \cap \dot{\bar{\mathfrak{s}}}(\{t_0, \ldots, t_{\Re}\}) = \dot{\bar{\mathfrak{s}}}(\mathbf{z} \cap \{t_0, \ldots, t_{\Re}\}) = \emptyset$, because $\dot{\bar{\mathfrak{s}}}$ agrees with $\dot{\mathfrak{s}}$ on $\{t_0, \ldots, t_{\Re}\}$, $\dot{\bar{\mathfrak{s}}}$ is injective and $\mathbf{z} \cap \{t_0, \ldots, t_{\Re}\} = \emptyset$, by (1). Finally, we prove the condition of Definition 23, namely that $\dot{\bar{\mathfrak{s}}}(\mathsf{roots}_{\mathsf{lhs}}(\forall_{\neg\mathfrak{h}} \mathbf{z} \,.\, \mathop{\Large *}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}))) \cap \mathrm{dom}(\mathfrak{h}) = \{\dot{\bar{\mathfrak{s}}}(\mathsf{root}(q_i(\mathbf{u}_i))) \mid i \in [\![1 \,..\, n]\!]\} \cap \{\dot{\bar{\mathfrak{s}}}(t_0)\} = \emptyset$. Suppose, for a contradiction, that this set is not empty, thus $\dot{\bar{\mathfrak{s}}}(t_0) = \dot{\bar{\mathfrak{s}}}(\mathsf{root}(q_i(\mathbf{u}_i)))$, for some $i \in [\![1 \,..\, n]\!]$. Because $\dot{\bar{\mathfrak{s}}}$ is injective, we have $t_0 = \mathsf{root}(q_i(\mathbf{u}_i))$. However, this contradicts with the condition $\mathop{\Large *}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \in \mathsf{Core}(\mathcal{P})$, which by Definition 19, requires that $\mathsf{root}(p(\mathbf{t})) \neq \mathsf{root}(q_i(\mathbf{u}_i))$, i.e., $t_0 \neq \mathsf{root}(q_i(\mathbf{u}_i))$.

"$\supseteq$" Let $\phi = \exists_{\mathfrak{h}} \overline{\mathbf{x}} \forall_{\neg\mathfrak{h}} \overline{\mathbf{y}} \,.\, \psi \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h})$ be a core formula, where ψ is quantifier-free. Note that, since $\phi \in \mathsf{Core}(\mathcal{P})$, we have $(\overline{\mathbf{x}} \cup \overline{\mathbf{y}}) \cap \mathcal{V}^1_{\mathcal{P}} = \emptyset$ because no variable in $\mathcal{V}^1_{\mathcal{P}}$ can be bound in ϕ; thus, since $\{t_0, \ldots, t_{\Re}\} \subseteq \mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C}$ by hypothesis, we have:

$$(\overline{\mathbf{x}} \cup \overline{\mathbf{y}}) \cap \{t_0, \ldots, t_{\Re}\} = \emptyset \;\; (\dagger).$$

By Definition 23, we have $(\dot{\bar{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \psi$, for some injective witness $\dot{\bar{\mathfrak{s}}} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}, \mathfrak{h}, \phi)$, such that $\dot{\bar{\mathfrak{s}}}(\overline{\mathbf{x}}) \subseteq \mathrm{loc}(\mathfrak{h})$ and $\dot{\bar{\mathfrak{s}}}(\overline{\mathbf{y}}) \cap \mathrm{loc}(\mathfrak{h}) = \emptyset$. Since $(\dot{\mathfrak{s}}, \mathfrak{h}) \models t_0 \mapsto (t_1, \ldots, t_{\Re})$, it must be the case that $\|\mathfrak{h}\| = 1$, hence ψ must be of either one of the forms:

- $v_0 \mapsto (v_1, \ldots, v_{\Re})$: in this case $\mathrm{dom}(\mathfrak{h}) = \{\dot{\bar{\mathfrak{s}}}(v_0)\}$ and $\mathfrak{h}(\dot{\bar{\mathfrak{s}}}(v_0)) = (\dot{\bar{\mathfrak{s}}}(v_1), \ldots, \dot{\bar{\mathfrak{s}}}(v_{\Re}))$, thus $\mathrm{loc}(\mathfrak{h}) = \{\dot{\bar{\mathfrak{s}}}(v_0), \ldots, \dot{\bar{\mathfrak{s}}}(v_{\Re})\}$. By $(\dagger)$, $\dot{\bar{\mathfrak{s}}}$ and $\dot{\mathfrak{s}}$ must agree over $t_0, \ldots, t_{\Re}$, hence we have $\dot{\bar{\mathfrak{s}}}(t_i) = \dot{\mathfrak{s}}(t_i)$, for all $i \in [\![0 \,..\, \Re]\!]$. Since $(\dot{\mathfrak{s}}, \mathfrak{h}) \models t_0 \mapsto (t_1, \ldots, t_{\Re})$, we obtain $\mathrm{dom}(\mathfrak{h}) = \{\dot{\mathfrak{s}}(t_0)\} = \{\dot{\bar{\mathfrak{s}}}(t_0)\}$ and $\mathfrak{h}(\dot{\mathfrak{s}}(t_0)) = (\dot{\mathfrak{s}}(t_1), \ldots, \dot{\mathfrak{s}}(t_{\Re})) = (\dot{\bar{\mathfrak{s}}}(t_1), \ldots, \dot{\bar{\mathfrak{s}}}(t_{\Re}))$. Since $\dot{\bar{\mathfrak{s}}}$ is injective, we obtain $v_i = t_i$, for all $i \in [\![0 \,..\, \Re]\!]$. By Definition 19, we have $\overline{\mathbf{x}} \cup \overline{\mathbf{y}} \subseteq \{t_0, \ldots, t_{\Re}\}$, thus $\overline{\mathbf{x}} = \overline{\mathbf{y}} = \emptyset$, by $(\dagger)$. Then we obtain $\phi = t_0 \mapsto (t_1, \ldots, t_{\Re})$ and $\phi \in F$ follows, by (1).
- $\mathop{\Large *}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$: Since $(\dot{\mathfrak{s}}, \mathfrak{h}) \models t_0 \mapsto (t_1, \ldots, t_{\Re})$, we have $\mathrm{loc}(\mathfrak{h}) = \{\dot{\mathfrak{s}}(t_0), \ldots, \dot{\mathfrak{s}}(t_{\Re})\}$. Since $\dot{\mathfrak{s}}$, $\dot{\bar{\mathfrak{s}}}$ agree over $\{t_0, \ldots, t_{\Re}\}$, we have $\mathrm{loc}(\mathfrak{h}) = \{\dot{\bar{\mathfrak{s}}}(t_0), \ldots, \dot{\bar{\mathfrak{s}}}(t_{\Re})\}$ and since $\dot{\bar{\mathfrak{s}}}(\overline{\mathbf{x}}) \subseteq \mathrm{loc}(\mathfrak{h})$ and $\dot{\bar{\mathfrak{s}}}$ is injective, the only possibility is $\overline{\mathbf{x}} = \emptyset$, so that $\phi = \forall_{\neg\mathfrak{h}} \overline{\mathbf{y}} \,.\, \mathop{\Large *}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$. Since $\forall_{\neg\mathfrak{h}} \overline{\mathbf{y}} \,.\, \mathop{\Large *}_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$ is a core formula, by Definition 19, we have $\overline{\mathbf{y}} \subseteq \mathbf{t} \cup \bigcup_{i=1}^{n} \mathbf{u}_i$ and therefore $\overline{\mathbf{y}} \subseteq \left(\mathbf{t} \cup \bigcup_{i=1}^{n} \mathbf{u}_i\right) \setminus (\{t_0, \ldots, t_{\Re}\} \cup \mathbb{C})$. Since $\mathrm{dom}(\dot{\mathfrak{s}}) = \{t_0, \ldots, t_{\Re}\} \cup \mathbb{C}$ and $\phi \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h})$, we have that $\mathsf{fv}(\phi) = \{t_0, \ldots, t_{\Re}\}$ and thus $\overline{\mathbf{y}} = \left(\mathbf{t} \cup \bigcup_{i=1}^{n} \mathbf{u}_i\right) \setminus (\{t_0, \ldots, t_{\Re}\} \cup \mathbb{C})$. Indeed, all variables $y \in \mathbf{t} \cup \bigcup_{i=1}^{n} \mathbf{u}_i$ not occurring in $\mathbf{y}$ necessarily occur in $\mathrm{dom}(\dot{\bar{\mathfrak{s}}}) \setminus \mathbf{y} = \mathrm{dom}(\dot{\mathfrak{s}})$. By (II), for each rule

$$p(\mathbf{x}) \Leftarrow_{\mathcal{S}} \exists \mathbf{w} \,.\, \psi * \mathop{\Large *}_{j=1}^{m} p_j(\mathbf{z}_j) \;\; (\dagger\dagger)$$

and each substitution $\tau : \mathbf{w} \rightharpoonup \mathbf{x} \cup \bigcup_{i=1}^{n} \mathbf{y}_i$, there exists a rule

$$\ast_{i=1}^{n} q_i(\mathbf{y}_i) \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{v} \,.\, \psi\tau \ast \ast_{j=1}^{m} \gamma_j \mathrel{-\!\!\bullet} p_j(\tau(\mathbf{z}_j)) \quad (\ddagger)$$

where $\ast_{j=1}^{m} \gamma_j = \ast_{i=1}^{n} q_i(\mathbf{y}_i)$ and $\mathbf{v} = \mathbf{w} \setminus \mathrm{dom}(\tau)$. Assume w.l.o.g. that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \ast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t})$ is a consequence of the above rule, i.e., that there exists a $\mathbf{v}$-associate $\mathfrak{s}'$ of $\dot{\mathfrak{s}}$ such that $(\mathfrak{s}', \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \psi\tau\sigma \ast \ast_{j=1}^{m} \gamma_j\sigma \mathrel{-\!\!\bullet} p_j(\sigma(\tau(\mathbf{z}_j)))$, where $\sigma \stackrel{\text{def}}{=} [\mathbf{t}/\mathbf{x}, \mathbf{u}_1/\mathbf{y}_1, \ldots, \mathbf{u}_n/\mathbf{y}_n]$. Since $\mathcal{S}$ is progressing, there is exactly one points-to atom in ψ and, because $\|\mathfrak{h}\| = 1$, it must be the case that $(\mathfrak{s}', \mathfrak{h}) \models \psi\tau\sigma$ and $(\mathfrak{s}', \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \gamma_j\sigma \mathrel{-\!\!\bullet} p_j(\sigma(\tau(\mathbf{z}_j)))$, for each $j \in [\![1 \,..\, m]\!]$. To prove that $\phi \in F$, it is sufficient to show the existence of a core unfolding $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} t_0 \mapsto (t_1, \ldots, t_{\Re}) \ast \ast_{i=1}^{n} \mathsf{emp} \mathrel{-\!\!\bullet} q_i(\mathbf{u}_i)$. To this end, we first prove the two points of Definition 21:

(1) Since $(\mathfrak{s}', \emptyset) \models_{\mathfrak{C}_{\mathcal{S}}} \gamma_j\sigma \mathrel{-\!\!\bullet} p_j(\sigma(\tau(\mathbf{z}_j)))$, for each $j \in [\![1 \,..\, m]\!]$, by Lemma 43, we obtain $\gamma_j\sigma = p_j(\mathbf{w}_j)$, for a tuple of variables $\mathbf{w}_j \in \mathrm{dom}(\mathfrak{s}')$, such that $\mathfrak{s}'(\mathbf{w}_j) = \mathfrak{s}'(\sigma(\tau(\mathbf{z}_j)))$. Since, moreover $\ast_{j=1}^{m} \gamma_j\sigma = \ast_{i=1}^{n} q_i(\mathbf{u}_i)$, we deduce that $n = m$ and, for each $i \in [\![1 \,..\, n]\!]$, we have $q_i = p_{j_i}$, for some $j_i \in [\![1 \,..\, m]\!]$. Then, by applying (II) to the rule (††), using the substitution τ, we obtain the rule:

$$\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{x}) \Leftarrow_{\mathfrak{C}_{\mathcal{S}}} \exists \mathbf{v} \,.\, \psi\tau \ast \ast_{i=1}^{n} \mathsf{emp} \mathrel{-\!\!\bullet} q_i(\tau(\mathbf{z}_{j_i})) \quad (\ddagger\ddagger)$$

(2) Let μ be the extension of σ with the pairs (z, u) such that $z \in \mathbf{v}$ and one of the following holds:

- if $\mathfrak{s}'(z) = \dot{\mathfrak{s}}(t_i)$, for some $i \in [\![0 \,..\, \Re]\!]$, then $u = t_i$,
- if $\mathfrak{s}'(z) = \dot{\mathfrak{s}}((\mathbf{u}_i)_\ell)$, for some $i \in [\![1 \,..\, n]\!]$ and $\ell \in [\![1 \,..\, \#q_i]\!]$, then $u = (\mathbf{u}_i)_\ell$,
- otherwise, $u = \min_{\preceq} \{v \in \mathbf{v} \mid \mathfrak{s}'(v) = \mathfrak{s}'(z)\}$, where $\preceq$ is a total order on $\mathbb{V}$.

Note that, since $\dot{\mathfrak{s}}$ is injective, for each $z \in \mathbf{v}$ there exist at most one pair $(z, u) \in \mu$ which is well-defined. Moreover, we have $\mu(\tau(\mathbf{z}_{j_i})) = \mathbf{u}_i$, because $\mathfrak{s}'(\sigma(\tau(\mathbf{z}_j))) = \mathfrak{s}'(\mathbf{u}_i) = \dot{\mathfrak{s}}(\mathbf{u}_i)$, for all $i \in [\![1 \,..\, n]\!]$. We now prove that

$$t_0 \mapsto (t_1, \ldots, t_{\Re}) \ast \ast_{i=1}^{n} \mathsf{emp} \mathrel{-\!\!\bullet} q_i(\mathbf{u}_i) \quad \in \quad \mathcal{T}\left(\psi\tau\mu \ast \ast_{i=1}^{n} \mathsf{emp} \mathrel{-\!\!\bullet} q_i(\mu(\tau(\mathbf{z}_{j_i})))\right)$$

or, equivalently, that $t_0 \mapsto (t_1, \ldots, t_{\Re}) \in \mathcal{T}(\psi\tau\mu)$. By a case split on the form of the atom α in $\psi\tau$, using the fact that $(\mathfrak{s}', \mathfrak{h}) \models \psi\tau\sigma$:

- $\alpha = u_1 \doteq u_2$: we have $\mathfrak{s}'(\sigma(u_1)) = \mathfrak{s}'(\sigma(u_2))$, hence $\mu(u_1) = \mu(u_2)$, by definition of μ and $\mathcal{T}(\alpha) = \{\mathsf{emp}\}$.
- $\alpha = u_1 \neq u_2$: we have $\mathfrak{s}'(\sigma(u_1)) \neq \mathfrak{s}'(\sigma(u_2))$, hence $\mu(u_1) \neq \mu(u_2)$, by definition of μ and $\mathcal{T}(\alpha) = \{\mathsf{emp}\}$.
- $\alpha = u_0 \mapsto (u_1, \ldots, u_{\Re})$: since $\mathcal{S}$ is progressing, α is the only points-to atom in ψ and $\mathrm{dom}(\mathfrak{h}) = \{\dot{\mathfrak{s}}(t_0)\} = \{\mathfrak{s}'(\sigma(u_0))\}$, $\mathfrak{h}(\dot{\mathfrak{s}}) = (\dot{\mathfrak{s}}(t_0), \ldots, \dot{\mathfrak{s}}(t_{\Re})) = (\mathfrak{s}'(\sigma(u_1)), \ldots, \mathfrak{s}'(\sigma(u_{\Re})))$. Then we obtain $\dot{\mathfrak{s}}(t_i) = \mathfrak{s}'(\sigma(u_i))$, hence $\mu(u_i) = t_i$, for all $i \in [\![0 \,..\, \Re]\!]$ and $\mathcal{T}(\alpha) = \{t_0 \mapsto (t_1, \ldots, t_{\Re})\}$.

We obtain the core unfolding $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} t_0 \mapsto (t_1, \ldots, t_{\Re}) \ast \ast_{i=1}^{n} \mathsf{emp} \mathrel{-\!\!\bullet} q_i(\mathbf{u}_i)$ and we are left with proving that $t_0 \notin \{\mathsf{root}(q_i(\mathbf{u}_i)) \mid i \in [\![1 \,..\, n]\!]\}$. By the definition of μ, there exists a points-to atom $u_0 \mapsto (u_1, \ldots, u_{\Re})$ in $\psi\tau$, such that $t_0 = \mu(u_0)$. Because $\mathcal{S}$ is progressing, it must be the case that $u_0 = \mathsf{root}(p(\mathbf{x}))$, hence $t_0 = \mathsf{root}(p(\mathbf{t}))$, by the definition of μ. Since ϕ is a core formula, by Definition 19, we obtain $\mathsf{root}(p(\mathbf{t})) \notin \{\mathsf{root}(q_i(\mathbf{u}_i)) \mid i \in [\![1 \,..\, n]\!]\}$ and we conclude that $\phi = \forall_{\neg \mathsf{h}} \overline{\mathbf{y}} \,.\, \ast_{i=1}^{n} q_i(\mathbf{u}_i) \mathrel{-\!\!\bullet} p(\mathbf{t}) \in F$, by (1). ◀

▶ **Lemma 54.** *If $\mathcal{S}$ is normalized, $\phi_1, \phi_2 \in \mathsf{SH}^{\Re}$ are symbolic heaps and $\langle(\dot{\mathfrak{s}}, \mathfrak{h}_1), (\dot{\mathfrak{s}}, \mathfrak{h}_2)\rangle$ is an injective normal $\mathcal{S}$-companion for (ϕ_1, ϕ_2), then:*

$$\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \cap \mathrm{dom}(\mathfrak{h}_1 \uplus \mathfrak{h}_2) \subseteq \dot{\mathfrak{s}}(\mathsf{alloc}_{\mathcal{S}}(\phi_1 \ast \phi_2) \cap (\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C})) \subseteq \mathrm{dom}(\mathfrak{h}_1 \uplus \mathfrak{h}_2).$$

Proof: Let $\ell \in \mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \cap \mathrm{dom}(\mathfrak{h}_1 \uplus \mathfrak{h}_2)$ be a location. By Lemma 36, since $\dot{\mathfrak{s}}$ is injective and $\mathbb{C} \subseteq \mathrm{dom}(\dot{\mathfrak{s}})$, we have $\ell \in \dot{\mathfrak{s}}(\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C})$. For $i = 1, 2$, let $\phi_i \Rightarrow_{\mathcal{S}}^{*} \exists \mathbf{x}_i \,.\, \psi_i$ be the predicate-free

unfolding and $\overline{\mathfrak{s}}_i$ be the $\mathbf{x}_i$-associate of $\dot{\mathfrak{s}}$ that satisfy points (1) and (2) of Definition 34. Assume that $\ell \in \mathrm{dom}(\mathfrak{h}_1)$ (the case $\ell \in \mathrm{dom}(\mathfrak{h}_2)$ is symmetric). Because $(\overline{\mathfrak{s}}_1, \mathfrak{h}_1) \models \psi_1$, there exists a points-to atom $t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}})$ in ψ_1, such that $\overline{\mathfrak{s}}_1(t_0) = \ell$. Since $\mathcal{S}$ is normalized, by Definition 9, the set $\mathsf{alloc}_{\mathcal{S}}(\phi_1)$ is well-defined and we distinguish two cases.

- If $t_0 \in \mathsf{alloc}_{\mathcal{S}}(\phi_1)$, then $\ell \in \dot{\mathfrak{s}}(\mathsf{alloc}_{\mathcal{S}}(\phi_1))$, because $\overline{\mathfrak{s}}_1$ and $\dot{\mathfrak{s}}$ agree over $\mathsf{alloc}_{\mathcal{S}}(\phi_1)$.
- Otherwise, we must have $t_0 \in \mathbf{x}_1$. Since $\ell \in \mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2)$, we have $\ell \in \mathrm{loc}(\mathfrak{h}_2)$, thus there exists a points-to atom $u_0 \mapsto (u_1, \ldots, u_{\mathfrak{K}})$ in ψ_2 such that $\ell = \overline{\mathfrak{s}}_2(u_i)$, for some $i \in [\![1 \,..\, \mathfrak{K}]\!]$. Note that $\ell = \overline{\mathfrak{s}}_2(u_0)$ is impossible, because $\ell \in \mathrm{dom}(\mathfrak{h}_1)$. Suppose, for a contradiction, that $\ell \notin \overline{\mathfrak{s}}(\mathbb{C})$. Then $u_i \in \mathsf{fv}(\psi_2)$ must be the case, which contradicts the condition $\overline{\mathfrak{s}}_1(\mathbf{x}_1) \cap \overline{\mathfrak{s}}_2(\mathsf{fv}(\psi_2)) \subseteq \overline{\mathfrak{s}}(\mathbb{C})$, required at point (2) of Definition 34. Hence $\ell \in \overline{\mathfrak{s}}(\mathbb{C})$ must be the case. Since $\ell = \overline{\mathfrak{s}}_1(t_0)$ either $t_0 \in \mathbb{C}$ or t_0 is an existentially allocated variable. The second case cannot occur, because of the Condition (2c) of Definition 8. Then we have $t_0 \in \mathbb{C}$ and, moreover, we have $t_0 \in \mathsf{alloc}_{\mathcal{S}}(\phi_1)$, by Definition 9, thus $t_0 \in \mathsf{alloc}_{\mathcal{S}}(\phi_1) \cap \mathbb{C}$.

In each case we obtain $\ell \in \overline{\mathfrak{s}}_1(\mathsf{alloc}_{\mathcal{S}}(\phi_1)) \cup \overline{\mathfrak{s}}_2(\mathsf{alloc}_{\mathcal{S}}(\phi_2)) \subseteq \dot{\mathfrak{s}}(\mathsf{alloc}_{\mathcal{S}}(\phi_1 * \phi_2))$, because $\overline{\mathfrak{s}}_i$ agrees with $\dot{\mathfrak{s}}$ over $\mathsf{alloc}_{\mathcal{S}}(\phi_i)$, for $i = 1, 2$. We obtain:

$$\begin{array}{rcl} \ell & \in & \dot{\mathfrak{s}}(\mathsf{alloc}_{\mathcal{S}}(\phi_1 * \phi_2)) \cap \dot{\mathfrak{s}}(\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C}) \\ & = & \dot{\mathfrak{s}}(\mathsf{alloc}_{\mathcal{S}}(\phi_1 * \phi_2) \cap (\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C})), \text{ because } \dot{\mathfrak{s}} \text{ is injective .} \end{array}$$

The second inclusion follows trivially from the fact that $\dot{\mathfrak{s}}(\mathsf{alloc}_{\mathcal{S}}(\phi_i)) \subseteq \mathrm{dom}(\mathfrak{h}_i)$, for $i = 1, 2$, which is an easy consequence of Definition 9. ◀

▶ **Lemma 55.** *Given an injective structure* $(\dot{\mathfrak{s}}, \mathfrak{h})$*, a variable* $x \notin \mathrm{dom}(\dot{\mathfrak{s}})$ *and a location* $\ell \notin \mathrm{loc}(\mathfrak{h}) \cup \mathrm{rng}(\dot{\mathfrak{s}})$*, we have* $C_{\mathcal{P}}(\dot{\mathfrak{s}}[x \leftarrow \ell], \mathfrak{h}) = \mathsf{add}(x, C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}))$.

Proof: "$\subseteq$" Let $\varphi = \exists_{\mathsf{h}} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \,.\, \phi \in C_{\mathcal{P}}(\dot{\mathfrak{s}}[x \leftarrow \ell], \mathfrak{h})$ be a core formula, where ϕ is quantifier-free. By Definition 23, there exists a witness $\dot{\overline{\mathfrak{s}}} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}[x \leftarrow \ell], \mathfrak{h}, \varphi)$, such that $\dot{\overline{\mathfrak{s}}}(\mathrm{roots}_{\mathsf{lhs}}(\varphi)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$. Let $\dot{\overline{\mathfrak{s}}}'$ be the store identical to $\dot{\overline{\mathfrak{s}}}$, except that $x \notin \mathrm{dom}(\dot{\overline{\mathfrak{s}}}')$ and $\dot{\overline{\mathfrak{s}}}'(\hat{x}) = \dot{\overline{\mathfrak{s}}}(x)$, for some variable $\hat{x} \notin \mathcal{V}^1_{\mathcal{P}}$. Since $\ell \notin \mathrm{loc}(\mathfrak{h})$, we have $\dot{\overline{\mathfrak{s}}}' \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}, \mathfrak{h}, \exists_{\mathsf{h}} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \forall_{\neg \mathsf{h}} \hat{x} \,.\, \phi[\hat{x}/x])$, because $\hat{x} \notin \mathcal{V}^1_{\mathcal{P}}$ we have $\exists_{\mathsf{h}} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \forall_{\neg \mathsf{h}} \hat{x} \,.\, \phi[\hat{x}/x] \in \mathsf{Core}(\mathcal{P})$, hence $\exists_{\mathsf{h}} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \forall_{\neg \mathsf{h}} \hat{x} \,.\, \phi[\hat{x}/x] \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h})$, from which we deduce that $\varphi \in \mathsf{add}(x, C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}))$.

"$\supseteq$" Let $\varphi = \exists_{\mathsf{h}} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \,.\, \phi \in \mathsf{add}(x, C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}))$, where ϕ is quantifier-free, and let $\psi = \exists_{\mathsf{h}} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \forall_{\neg \mathsf{h}} \hat{x} \,.\, \phi[\hat{x}/x]$. By (3), we have $\psi \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h})$. By Definition 23, there exists a witness $\dot{\overline{\mathfrak{s}}} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}, \mathfrak{h}, \psi)$, such that $\dot{\overline{\mathfrak{s}}}(\mathrm{roots}_{\mathsf{lhs}}(\psi)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$. W.l.o.g., by Lemma 51, we can assume that $\dot{\overline{\mathfrak{s}}}$ is such that $\ell \neq \dot{\overline{\mathfrak{s}}}(y)$, for all $y \in \mathrm{dom}(\dot{\overline{\mathfrak{s}}})$ such that $\dot{\overline{\mathfrak{s}}}(y) \notin \mathrm{loc}(\mathfrak{h})$. With this assumption, $\dot{\overline{\mathfrak{s}}}[x \leftarrow \ell]$ is injective. We prove that $\dot{\overline{\mathfrak{s}}}[x \leftarrow \ell] \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}[x \leftarrow \ell], \mathfrak{h}, \varphi)$:

- Let $\dot{\overline{\mathfrak{s}}}'$ be the store identical to $\dot{\overline{\mathfrak{s}}}[x \leftarrow \ell]$ except that the images of x and $\hat{x}$ are switched. Since $(\dot{\overline{\mathfrak{s}}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi[\hat{x}/x]$ we have $(\dot{\overline{\mathfrak{s}}}', \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi$. Since $\dot{\overline{\mathfrak{s}}}(x), \ell \notin \mathrm{loc}(\mathfrak{h})$ (as $\dot{\overline{\mathfrak{s}}}(x) = \dot{\mathfrak{s}}(\hat{x})$, by definition, and $\dot{\mathfrak{s}}(\hat{x}) \notin \mathrm{loc}(\mathfrak{h})$, by Condition (3) of Definition 23), we have $\dot{\overline{\mathfrak{s}}}' \approx_{\mathrm{loc}(\mathfrak{h})} \dot{\overline{\mathfrak{s}}}[x \leftarrow \ell]$ thus $(\dot{\overline{\mathfrak{s}}}[\hat{x} \leftarrow \ell], \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi$, by Lemma 51.
- Since $x \notin \mathbf{x}$, we have $\dot{\overline{\mathfrak{s}}}[x \leftarrow \ell](\mathbf{x}) = \dot{\overline{\mathfrak{s}}}(\mathbf{x}) \subseteq \mathrm{loc}(\mathfrak{h})$.
- Since $\ell \notin \mathrm{loc}(\mathfrak{h})$ and $\dot{\overline{\mathfrak{s}}}(\mathbf{y}) \cap \mathrm{loc}(\mathfrak{h}) = \emptyset$, we have $\dot{\overline{\mathfrak{s}}}[x \leftarrow \ell](\mathbf{y}) \cap \mathrm{loc}(\mathfrak{h}) = \emptyset$.

Since $\mathrm{roots}_{\mathsf{lhs}}(\exists_{\mathsf{h}} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \forall_{\neg \mathsf{h}} \hat{x} \,.\, \phi[\hat{x}/x]) = \mathrm{roots}_{\mathsf{lhs}}(\varphi)$, we have $\dot{\overline{\mathfrak{s}}}(\mathrm{roots}_{\mathsf{lhs}}(\varphi)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$, thus $\dot{\overline{\mathfrak{s}}}[x \leftarrow \ell] \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}[x \leftarrow \ell], \mathfrak{h}, \varphi)$, which implies $\varphi \in C_{\mathcal{P}}(\dot{\mathfrak{s}}[x \leftarrow \ell], \mathfrak{h})$. ◀

▶ **Lemma 56.** *Given an injective structure* $(\dot{\mathfrak{s}}, \mathfrak{h})$ *and a variable* $x \in \mathrm{dom}(\dot{\mathfrak{s}}) \cap \mathcal{V}^1_{\mathcal{P}}$ *such that* $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h})$*, we have* $C_{\mathcal{P}}(\dot{\mathfrak{s}}', \mathfrak{h}) = \mathsf{rem}(x, C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}))$*, where* $\dot{\mathfrak{s}}'$ *is the restriction of* $\dot{\mathfrak{s}}$ *to* $\mathrm{dom}(\dot{\mathfrak{s}}) \setminus \{x\}$.

Proof: First note that because $\dot{\mathfrak{s}}$ is injective, $\dot{\mathfrak{s}}'$ is necessarily injective, thus $C_{\mathcal{P}}(\dot{\mathfrak{s}}', \mathfrak{h})$ is well defined. We prove both inclusions.

"$\subseteq$" Let $\varphi = \exists_{\mathsf{h}}\mathbf{x}\forall_{\neg\mathsf{h}}\mathbf{y}\,.\,\phi \in C_{\mathcal{P}}(\dot{\mathsf{s}}',\mathsf{h})$ be a core formula, where ϕ is quantifier-free. By Definition 23, there exists a witness $\dot{\overline{\mathsf{s}}}' \in \mathcal{W}_{\mathcal{S}}(\dot{\mathsf{s}}',\mathsf{h},\varphi)$, such that $\dot{\overline{\mathsf{s}}}'(\mathsf{roots}_{\mathsf{lhs}}(\varphi)) \cap \mathrm{dom}(\mathsf{h}) = \emptyset$. Since $x \notin \mathrm{dom}(\dot{\mathsf{s}}')$ and $(\dot{\mathsf{s}}',\mathsf{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \varphi$, we have $x \notin \mathsf{fv}(\varphi)$. By α-renaming if necessary, we can assume w.l.o.g. that $x \notin \mathbf{x} \cup \mathbf{y}$ (†). This is possible since $x \in \mathcal{V}^1_{\mathcal{P}}$, hence if $x \in \mathbf{x} \cup \mathbf{y}$ then by definition of $\mathsf{Core}(\mathcal{P})$ it cannot occur in $\mathrm{roots}(\phi)$; it can therefore be renamed by a variable not occurring in $\mathcal{V}^1_{\mathcal{P}}$. We distinguish the following cases.

- If $\dot{\mathsf{s}}(x) \neq \dot{\overline{\mathsf{s}}}'(x')$ for all $x' \in \mathbf{x}$, then $\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)]$ is an injective associate of $\dot{\overline{\mathsf{s}}}'$: indeed, by hypothesis, $\dot{\mathsf{s}}(x) \in \mathrm{loc}(\mathsf{h})$ and $\dot{\overline{\mathsf{s}}}'(\mathbf{y}) \cap \mathrm{loc}(\mathsf{h}) = \emptyset$, thus $\dot{\mathsf{s}}(x) \notin \dot{\overline{\mathsf{s}}}'(\mathbf{y})$. Since ϕ is quantifier-free and $\dot{\overline{\mathsf{s}}}'$ agrees with $\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)]$ on $\mathsf{fv}(\phi)$, we obtain $(\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)],\mathsf{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi$. We now prove that $\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)] \in \mathcal{W}_{\mathcal{S}}(\dot{\mathsf{s}},\mathsf{h},\varphi)$, which suffices to show $\varphi \in C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h})$, by the definition of the latter set:
  - $\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)](\mathbf{x}) \subseteq \dot{\overline{\mathsf{s}}}'(\mathbf{x}) \cup \{\dot{\mathsf{s}}(x)\} \subseteq \mathrm{loc}(\mathsf{h})$, because $\dot{\overline{\mathsf{s}}}' \in \mathcal{W}_{\mathcal{S}}(\dot{\mathsf{s}}',\mathsf{h},\varphi)$ and $\dot{\mathsf{s}}(x) \in \mathrm{loc}(\mathsf{h})$ by hypothesis.
  - $\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)](\mathbf{y}) = \dot{\overline{\mathsf{s}}}'(\mathbf{y})$ and $\dot{\overline{\mathsf{s}}}'(\mathbf{y}) \cap \mathrm{loc}(\mathsf{h}) = \emptyset$, because $\dot{\overline{\mathsf{s}}}' \in \mathcal{W}_{\mathcal{S}}(\dot{\mathsf{s}}',\mathsf{h},\varphi)$.
  - $\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)](\mathsf{roots}_{\mathsf{lhs}}(\varphi)) = \dot{\overline{\mathsf{s}}}'(\mathsf{roots}_{\mathsf{lhs}}(\varphi))$ because $x \notin \mathsf{fv}(\phi)$, and $\dot{\overline{\mathsf{s}}}'(\mathsf{roots}_{\mathsf{lhs}}(\varphi)) \cap \mathrm{dom}(\mathsf{h}) = \emptyset$ because $\dot{\overline{\mathsf{s}}}' \in \mathcal{W}_{\mathcal{S}}(\dot{\mathsf{s}}',\mathsf{h},\varphi)$.

  Consequently we obtain $\varphi \in C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h})$, and since $x \notin \mathsf{fv}(\varphi)$, we have $C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h}) \subseteq \mathsf{rem}(x, C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h}))$, hence the result.
- Otherwise, $\dot{\mathsf{s}}(x) = \dot{\overline{\mathsf{s}}}'(x')$ for some $x' \in \mathbf{x}$, hence φ is of the form $\exists_{\mathsf{h}}x'\exists_{\mathsf{h}}\mathbf{x}'\forall_{\neg\mathsf{h}}\mathbf{y}\,.\,\phi$, where $\mathbf{x}' \stackrel{\text{def}}{=} \mathbf{x} \setminus \{x'\}$. Clearly, the variable x' must be unique, otherwise $\dot{\overline{\mathsf{s}}}'$ would not be injective. Let $\dot{\overline{\mathsf{s}}}$ be the injective store obtained from $\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)]$ by removing the pair $(x', \dot{\mathsf{s}}(x))$ from it. We prove that $\dot{\overline{\mathsf{s}}} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathsf{s}},\mathsf{h},\exists_{\mathsf{h}}\mathbf{x}'\forall_{\neg\mathsf{h}}\mathbf{y}\,.\,\phi[x/x'])$:
  - $(\dot{\overline{\mathsf{s}}},\mathsf{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi[x/x']$, because $\dot{\overline{\mathsf{s}}}$ agrees with $\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)]$ on $\mathsf{fv}(\phi[x/x'])$.
  - $\dot{\overline{\mathsf{s}}}(\mathbf{x}') = \dot{\overline{\mathsf{s}}}'(\mathbf{x}') \subseteq \mathrm{loc}(\mathsf{h})$, because $\dot{\overline{\mathsf{s}}}' \in \mathcal{W}_{\mathcal{S}}(\dot{\mathsf{s}}',\mathsf{h},\varphi)$.
  - $\dot{\overline{\mathsf{s}}}(\mathbf{y}) = \dot{\overline{\mathsf{s}}}'(\mathbf{y})$, because $x \notin \mathbf{y}$ (†) and $\dot{\overline{\mathsf{s}}}'(\mathbf{y}) \cap \mathrm{loc}(\mathsf{h}) = \emptyset$, because $\dot{\overline{\mathsf{s}}}' \in \mathcal{W}_{\mathcal{S}}(\dot{\mathsf{s}}',\mathsf{h},\varphi)$.

  Furthermore, we have $\dot{\overline{\mathsf{s}}}'[x \leftarrow \dot{\mathsf{s}}(x)](\mathsf{roots}_{\mathsf{lhs}}(\varphi)) = \dot{\overline{\mathsf{s}}}'(\mathsf{roots}_{\mathsf{lhs}}(\varphi))$ because $x \notin \mathsf{fv}(\varphi)$, hence $x \notin \mathsf{roots}_{\mathsf{lhs}}(\varphi)$. Thus $\dot{\overline{\mathsf{s}}}(\mathsf{roots}_{\mathsf{lhs}}(\varphi)) \subseteq \dot{\overline{\mathsf{s}}}'(\mathsf{roots}_{\mathsf{lhs}}(\varphi))$ and, since $\dot{\overline{\mathsf{s}}}'(\mathsf{roots}_{\mathsf{lhs}}(\varphi)) \cap \mathrm{dom}(\mathsf{h}) = \emptyset$ by Definition 23, we deduce that $\dot{\overline{\mathsf{s}}}(\mathsf{roots}_{\mathsf{lhs}}(\varphi)) \cap \mathrm{dom}(\mathsf{h}) = \emptyset$. Still by Definition 23, we obtain that $\exists_{\mathsf{h}}\mathbf{x}'\forall_{\neg\mathsf{h}}\mathbf{y}\,.\,\phi[x/x'] \in C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h})$ and thus $\exists_{\mathsf{h}}x'\exists_{\mathsf{h}}\mathbf{x}'\forall_{\neg\mathsf{h}}\mathbf{y}\,.\,\phi \in \mathsf{rem}(x, C_{\mathcal{P}}(\dot{\mathsf{s}}))$ (with $\hat{x} \stackrel{\text{def}}{=} x'$).

"$\supseteq$" Let $\varphi = \exists_{\mathsf{h}}\mathbf{x}\forall_{\neg\mathsf{h}}\mathbf{y}\,.\,\phi \in \mathsf{rem}(x, C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h}))$, for some quantifier-free formula ϕ. We distinguish the following cases.

- If $\varphi \in C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h})$ and $x \notin \mathsf{fv}(\varphi)$, then for any injective structure $(\dot{\mathsf{s}},\mathsf{h})$ meeting the conditions of Definition 23, the structure $(\dot{\mathsf{s}}',\mathsf{h})$ is injective and trivially meets the conditions of Definition 23, hence $\varphi \in C_{\mathcal{P}}(\dot{\mathsf{s}}',\mathsf{h})$.
- Otherwise, $\varphi = \exists_{\mathsf{h}}\hat{x}\exists_{\mathsf{h}}\mathbf{x}'\forall_{\neg\mathsf{h}}\mathbf{y}\,.\phi[\hat{x}/x]$, $x \in \mathsf{fv}(\exists_{\mathsf{h}}\mathbf{x}'\forall_{\neg\mathsf{h}}\mathbf{y}\,.\phi)$ and $\exists_{\mathsf{h}}\mathbf{x}'\forall_{\neg\mathsf{h}}\mathbf{y}\,.\phi \in C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h})$, where $\mathbf{x}' \stackrel{\text{def}}{=} \mathbf{x} \setminus \{x\}$. Let $\dot{\overline{\mathsf{s}}}$ be an injective $(\mathbf{x}' \cup \mathbf{y})$-associate of $\dot{\mathsf{s}}$ meeting the conditions from Definition 23. It is easy to check that $(\dot{\overline{\mathsf{s}}} \setminus \{(x, \dot{\overline{\mathsf{s}}}(x))\}) \cup \{(\hat{x}, \dot{\overline{\mathsf{s}}}(x))\} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathsf{s}},\mathsf{h},\varphi)$, thus $\varphi \in C_{\mathcal{P}}(\dot{\mathsf{s}}',\mathsf{h})$. ◀

K Proof of Lemma 27 (Section 6)

By induction on the structure of $\mathcal{F}_{\mathcal{P}}$, defined as the least set satisfying the constraints (1), (2), (3) and (4), we prove that $(\dot{\mathsf{s}},\mathsf{h})$ is an injective normal $\mathfrak{C}_{\mathcal{S}}$-model of ϕ if and only if $(\phi, C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h})) \in \mathcal{F}_{\mathcal{P}}$. Based on the structure of the core formula $\phi \in \mathcal{T}(\varphi)$, for some symbolic heap $\varphi \in \mathsf{SH}^{\mathfrak{K}}$, we distinguish the following cases:

- $\phi = t_0 \mapsto (t_1,\ldots,t_{\mathfrak{K}})$: because $\mathcal{S}$ is progressing, by Lemma 53, we obtain that $(\phi, F) \in \mathcal{F}_{\mathcal{P}}$ if and only if $F = C_{\mathcal{P}}(\dot{\mathsf{s}},\mathsf{h})$, for some injective $\mathcal{S}$-model $(\dot{\mathsf{s}},\mathsf{h})$ of $t_0 \mapsto (t_1,\ldots,t_{\mathfrak{K}})$, such that $\mathrm{dom}(\dot{\mathsf{s}}) = \{t_0,\ldots,t_{\mathfrak{K}}\} \cup \mathbb{C}$. Since any injective $\mathcal{S}$-model $(\dot{\mathsf{s}},\mathsf{h})$ of $t_0 \mapsto (t_1,\ldots,t_{\mathfrak{K}})$ is also normal, we conclude this case.
- $\phi = \mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$: "$\Rightarrow$" Since $\mathcal{F}_{\mathcal{P}}$ is the least relation satisfying (2), $(\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}), F) \in \mathcal{F}_{\mathcal{P}}$ if and

only if $(\exists_{\mathsf{h}}\mathbf{y}\,.\,\psi, F) \in \mathcal{F}_{\mathcal{P}}$, for some core unfolding $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} \psi$, where $\mathbf{y} = \mathsf{fv}(\psi) \setminus \mathbf{t}$. By the induction hypothesis, there exists an injective normal $\mathfrak{C}_{\mathcal{S}}$-model $(\dot{\mathsf{s}}, \mathfrak{h})$ of $\exists_{\mathsf{h}}\mathbf{y}\,.\,\psi$ such that $F = C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h})$ and $\mathrm{dom}(\dot{\mathsf{s}}) = \mathsf{fv}(\exists_{\mathsf{h}}\mathbf{y}\,.\,\psi) \cup \mathbb{C}$. Since $\mathcal{P}$ is normalized, by Condition 1b in Definition 8 we have $\mathsf{fv}(\exists_{\mathsf{h}}\mathbf{y}\,.\,\psi) = \mathsf{fv}(\phi)$. By Lemma 48, $(\dot{\mathsf{s}}, \mathfrak{h})$ is an injective $\mathfrak{C}_{\mathcal{S}}$-model of $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$. Because ϕ is quantifier-free, $(\dot{\mathsf{s}}, \mathfrak{h})$ is also an injective normal $\mathfrak{C}_{\mathcal{S}}$-model of ϕ. "$\Leftarrow$" Let $(\dot{\mathsf{s}}, \mathfrak{h})$ be an injective normal $\mathfrak{C}_{\mathcal{S}}$-model of $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$. By Lemma 48, there exists a core unfolding $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}) \rightsquigarrow_{\mathfrak{C}_{\mathcal{S}}} \psi$ and an injective extension $\dot{\bar{\mathsf{s}}}$ of $\dot{\mathsf{s}}$, such that $(\dot{\bar{\mathsf{s}}}, \mathfrak{h})$ is an injective $\mathfrak{C}_{\mathcal{S}}$-model of ψ. Let $\mathbf{y} \stackrel{\text{def}}{=} \mathsf{fv}(\psi) \setminus \mathbf{t}$. Then every variable $x \in \mathbf{y}$ occurs in a points-to or a predicate atom, by Definition 21. Since $\mathcal{S}$ is normalized, we obtain that $\dot{\bar{\mathsf{s}}}(x) \in \mathrm{loc}(\mathfrak{h})$, by point (2a) of Definition 8, and therefore $(\dot{\mathsf{s}}, \mathfrak{h})$ is an injective $\mathfrak{C}_{\mathcal{S}}$-model of $\exists_{\mathsf{h}}\mathbf{y}\,.\,\psi$. Since ψ is satisfiable, it cannot contain two atoms with the same root. We have $\mathsf{fv}(\psi) = \mathsf{fv}(\phi) \subseteq \mathcal{V}^1_{\mathcal{P}}$. Furthermore, since $\|\mathcal{V}^2_{\mathcal{P}}\| = \mathrm{width}(\mathcal{P})$ and $\mathrm{size}(\psi) \leq \mathrm{width}(\mathcal{P})$, we can assume w.l.o.g. that $\mathbf{y} \subseteq \mathcal{V}^2_{\mathcal{P}}$, hence $\exists_{\mathsf{h}}\mathbf{y}\,.\,\psi$ is a core formula. By the induction hypothesis, we obtain that $\langle \exists_{\mathsf{h}}\mathbf{y}\,.\,\psi, C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h})\rangle \in \mathcal{F}_{\mathcal{P}}$, thus $\langle \mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t}), C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h})\rangle \in \mathcal{F}_{\mathcal{P}}$ follows, by (2).

- $\phi = \phi_1 * \phi_2$: "$\Rightarrow$" Since $\mathcal{F}_{\mathcal{P}}$ is the least set satisfying (3), $(\phi_1 * \phi_2, F) \in \mathcal{F}_{\mathcal{P}}$ if and only if $(\phi_i, F_i) \in \mathcal{F}_{\mathcal{P}}$ and $F = \mathsf{add}(X_1, F_1) \circledast_D \mathsf{add}(X_2, F_2)$, where $X_i = \mathsf{fv}(\phi_i) \setminus \mathsf{fv}(\phi_{3-i})$, for $i = 1, 2$, $\mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_1) \cap \mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_2) = \emptyset$ and $D = \mathsf{alloc}_{\mathcal{S}}(\phi_1 * \phi_2) \cap (\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C})$. Since $\mathsf{fv}(\phi_i) \subseteq \mathsf{fv}(\phi) \subseteq \mathcal{V}^1_{\mathcal{P}}$, by the inductive hypothesis, there exist injective normal $\mathfrak{C}_{\mathcal{S}}$-models $(\dot{\mathsf{s}}_i, \mathfrak{h}_i)$ of ϕ_i, such that $F_i = C_{\mathcal{P}}(\dot{\mathsf{s}}_i, \mathfrak{h}_i)$, for $i = 1, 2$. By renaming locations if necessary, we assume w.l.o.g. that $\dot{\mathsf{s}}_1$ and $\dot{\mathsf{s}}_2$ agree over $\mathsf{trm}(\phi_1) \cap \mathsf{trm}(\phi_2)$ and that $\dot{\mathsf{s}}_i(\mathsf{fv}(\phi_i) \setminus \mathsf{fv}(\phi_{3-i})) \cap (\dot{\mathsf{s}}_{3-i}(\mathsf{fv}(\phi_{3-i}) \setminus \mathsf{fv}(\phi_i)) \cup \mathrm{loc}(\mathfrak{h}_{3-i})) = \emptyset$, for $i = 1, 2$ (†). This is feasible since the truth value of formulæ does not depend on the name of the locations. Let $\dot{\mathsf{s}} = \dot{\mathsf{s}}_1 \cup \dot{\mathsf{s}}_2$. It is easy to check that $\langle(\dot{\mathsf{s}}, \mathfrak{h}_1), (\dot{\mathsf{s}}, \mathfrak{h}_2)\rangle$ is an injective normal $\mathfrak{C}_{\mathcal{S}}$-companion for (ϕ_1, ϕ_2), by Definition 34. Moreover, by Lemma 55, we have $C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h}_i) = \mathsf{add}(X_i, F_i)$, for $i = 1, 2$. Next, we prove that $\mathfrak{h}_1$ and $\mathfrak{h}_2$ are disjoint heaps. Suppose, for a contradiction, that $\mathrm{dom}(\mathfrak{h}_1) \cap \mathrm{dom}(\mathfrak{h}_2) \neq \emptyset$. By assumption (†), there exists a variable $x \in \mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2)$, such that $\dot{\mathsf{s}}(x) \in \mathrm{dom}(\mathfrak{h}_1) \cap \mathrm{dom}(\mathfrak{h}_2)$. Since $\mathcal{P}$ is normalized, by Conditions (2b) and (2c) in Definition 8, the only variables that can be allocated by a model of a core formula ϕ_i are $\mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_i)$, we must have $x \in \mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_1) \cap \mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_2)$, which contradicts with the condition that $\mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_1) \cap \mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_2) = \emptyset$. We conclude that $\mathfrak{h}_1$ and $\mathfrak{h}_2$ are disjoint and let $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$. By Lemmas 36 and 54, we respectively have $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \subseteq \dot{\mathsf{s}}(\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C}) \subseteq \dot{\mathsf{s}}(\mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C})$ and $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \cap \mathrm{dom}(\mathfrak{h}) \subseteq \dot{\mathsf{s}}(D) \subseteq \mathrm{dom}(\mathfrak{h})$. Thus $(\dot{\mathsf{s}}, \mathfrak{h})$ is an injective normal $\mathfrak{C}_{\mathcal{S}}$-model of $\phi_1 * \phi_2$ and, by Definition 26, we have $C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h}) = C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h}_1) \circledast_D C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h}_2) = \mathsf{add}(X_1, F_1) \circledast_D \mathsf{add}(X_2, F_2)$.
  "$\Leftarrow$" Let $(\dot{\mathsf{s}}, \mathfrak{h})$ be an injective normal $\mathfrak{C}_{\mathcal{S}}$-model of $\phi_1 * \phi_2$. Note that since $\phi_1 * \phi_2$ is satisfiable we must have $\mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_1) \cap \mathsf{alloc}_{\mathfrak{C}_{\mathcal{S}}}(\phi_2) = \emptyset$. By Lemma 35, there exists an injective $\mathfrak{C}_{\mathcal{S}}$-normal companion $\langle(\dot{\mathsf{s}}_1, \mathfrak{h}_1), (\dot{\mathsf{s}}_2, \mathfrak{h}_2)\rangle$ for (ϕ_1, ϕ_2), such that $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$. Since $(\dot{\mathsf{s}}_i, \mathfrak{h}_i)$ is an injective normal $\mathfrak{C}_{\mathcal{S}}$-model of ϕ_i, we have $\langle \phi_i, C_{\mathcal{P}}(\dot{\mathsf{s}}_i, \mathfrak{h}_i)\rangle \in \mathcal{F}_{\mathcal{P}}$, by the inductive hypothesis, for $i = 1, 2$. We prove that $\dot{\mathsf{s}}(X_i) \cap \mathrm{loc}(\mathfrak{h}_i) = \emptyset$, where $X_i \stackrel{\text{def}}{=} \mathsf{fv}(\phi_i) \setminus \mathsf{fv}(\phi_{3-i})$, for $i = 1, 2$. Let $i = 1$, the case $i = 2$ being symmetric, and suppose, for a contradiction, that $\dot{\mathsf{s}}(x) \in \mathrm{loc}(\mathfrak{h}_1)$, for some $x \in X_1$. Because $\mathcal{S}$ is normalized, by point (2a) of Definition 8, we have $\dot{\mathsf{s}}(x) \in \mathrm{loc}(\mathfrak{h}_2)$, thus $\dot{\mathsf{s}}(x) \in \mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2)$. By Lemma 36, $\dot{\mathsf{s}}(x) \subseteq \dot{\mathsf{s}}(\mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C}$ and, since $\dot{\mathsf{s}}$ is injective, we deduce that $x \in \mathsf{fv}(\phi_1) \cap \mathsf{fv}(\phi_2) \cup \mathbb{C}$, which contradicts the hypothesis that $x \in X_1$. Hence $\dot{\mathsf{s}}(X_i) \cap \mathrm{loc}(\mathfrak{h}_i) = \emptyset$ and, by Lemma 55, we obtain $C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h}_i) = \mathsf{add}(X_i, C_{\mathcal{P}}(\dot{\mathsf{s}}_i, \mathfrak{h}_i))$, for $i = 1, 2$. Moreover, by Lemmas 36 and 54, we respectively have $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \subseteq \dot{\mathsf{s}}(\mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C})$ and $\mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \cap \mathrm{dom}(\mathfrak{h}) \subseteq \dot{\mathsf{s}}(D) \subseteq \mathrm{dom}(\mathfrak{h})$. By Definition 26, we have $C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h}) = \mathsf{add}(X_1, C_{\mathcal{P}}(\dot{\mathsf{s}}_1, \mathfrak{h}_1)) \circledast_D \mathsf{add}(X_2, C_{\mathcal{P}}(\dot{\mathsf{s}}_2, \mathfrak{h}_2))$, thus $\langle \phi_1 * \phi_2, C_{\mathcal{P}}(\dot{\mathsf{s}}, \mathfrak{h})\rangle \in \mathcal{F}_{\mathcal{P}}$, by (3).
- $\exists_{\mathsf{h}} x' \,.\, \phi'_1$: By α-renaming if necessary, we assume that $x' \in \mathcal{V}^2_{\mathcal{P}}$. Note that this is possible because $\|\mathcal{V}^2_{\mathcal{P}}\| \geq \mathrm{size}(\phi'_1)$. Furthermore, since we also have $\|\mathcal{V}^1_{\mathcal{P}}\| \geq \mathrm{size}(\phi'_1)$, we may assume that there exists a variable $x \in \mathcal{V}^1_{\mathcal{P}} \setminus \mathsf{fv}(\phi'_1)$. It is clear that $\phi_1 = \phi'_1[x/x']$ is a core formula. "$\Rightarrow$" Since $\mathcal{F}_{\mathcal{P}}$ is the least relation satisfying (4), we have $(\exists_{\mathsf{h}} x' \,.\, \phi'_1,\ F) \in \mathcal{F}_{\mathcal{P}}$ only if there exists a set of core

formulæ $F_1 \subseteq \mathsf{Core}(\mathcal{P})$, such that $F = \mathsf{rem}(x, F_1)$ and $(\phi_1, F_1) \in \mathcal{F}_\mathcal{P}$. By the inductive hypothesis, there exists an injective normal $\mathfrak{C}_\mathcal{S}$-model $(\dot{\mathfrak{s}}_1, \mathfrak{h})$ of ϕ_1 such that $F_1 = C_\mathcal{P}(\dot{\mathfrak{s}}_1, \mathfrak{h})$. By Lemma 56, we obtain $F = C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h})$, where $\dot{\mathfrak{s}}$ is the restriction of $\dot{\mathfrak{s}}_1$ to $\mathrm{dom}(\dot{\mathfrak{s}}_1) \setminus \{x\}$. Since $\mathcal{S}$ is normalized and the only occurrences of predicate atoms in ϕ_1 are of the form $\mathsf{emp} \mathrel{-\!\!\bullet} p(\mathbf{t})$, we have $\dot{\mathfrak{s}}_1(x) \in \mathrm{loc}(\mathfrak{h})$. Thus we conclude by noticing that $(\dot{\mathfrak{s}}, \mathfrak{h})$ is an injective normal $\mathfrak{C}_\mathcal{S}$-model of $\exists_\mathfrak{h} x' \,.\, \phi_1'$. "$\Leftarrow$" Let $(\dot{\mathfrak{s}}, \mathfrak{h})$ be an injective normal $\mathfrak{C}_\mathcal{S}$-model of $\exists_\mathfrak{h} x' \,.\, \phi_1'$, with $\mathrm{dom}(\dot{\mathfrak{s}}) = (\mathsf{fv}(\phi_1) \setminus \{x\}) \cup \mathbb{C}$. There exists $\ell \in \mathrm{loc}(\mathfrak{h}) \setminus \mathrm{rng}(\dot{\mathfrak{s}})$ such that $(\dot{\mathfrak{s}}[x \leftarrow \ell], \mathfrak{h})$ is an injective normal $\mathfrak{C}_\mathcal{S}$-model of ϕ_1. Since $\dot{\mathfrak{s}}[x \leftarrow \ell]$ is an injective extension of $\dot{\mathfrak{s}}$ and $\ell \in \mathrm{loc}(\mathfrak{h})$, by Lemma 56, $C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h}) = \mathsf{rem}(x, C_\mathcal{P}(\dot{\mathfrak{s}}[x \leftarrow \ell], \mathfrak{h}))$ and $(\exists_\mathfrak{h} x' \,.\, \phi_1',\ F) \in \mathcal{F}_\mathcal{P}$ follows, by the inductive hypothesis. ◀

We prove below that $\Vdash$ is a logical consequence relation:

▶ **Lemma 57.** *If $\phi \Vdash^* \psi$ then $\phi \models_{\mathfrak{C}_\mathcal{S}} \psi$.*

Proof: The proof is by induction on the length $n \geq 0$ of the derivation sequence from ϕ to ψ. If $n = 0$ then $\phi = \psi$ and there is nothing to prove. Assume $n = 1$, the case $n > 1$ follows immediately by the inductive hypothesis. We assume that $\phi = [\alpha \mathrel{-\!\!\bullet} p(\mathbf{t})] * [(\beta * p(\mathbf{t})) \mathrel{-\!\!\bullet} q(\mathbf{u})]$ and $\psi = (\alpha * \beta) \mathrel{-\!\!\bullet} q(\mathbf{u})$, for some predicate atoms $p(\mathbf{t})$ and $q(\mathbf{u})$ and some possibly empty conjunctions of predicate atoms α and β. Then there exist two disjoint heaps $\mathfrak{h}_1$ and $\mathfrak{h}_2$, such that $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$, $(\mathfrak{s}, \mathfrak{h}_1) \models_{\mathfrak{C}_\mathcal{S}} \alpha \mathrel{-\!\!\bullet} p(\mathbf{t})$ and $(\mathfrak{s}, \mathfrak{h}_2) \models_{\mathfrak{C}_\mathcal{S}} (\beta * p(\mathbf{t})) \mathrel{-\!\!\bullet} q(\mathbf{u})$. We prove that $(\mathfrak{s}, \mathfrak{h}) \models \psi$ by induction on $\|\mathfrak{h}_2\|$. If $\|\mathfrak{h}_2\| = 0$ then $\beta = \mathsf{emp}$ and, by Lemma 43, we obtain $p = q$ and $\mathfrak{s}(\mathbf{t}) = \mathfrak{s}(\mathbf{u})$. Thus $\mathfrak{h} = \mathfrak{h}_1$ and $(\mathfrak{s}, \mathfrak{h}) \models (\alpha * \beta) \mathrel{-\!\!\bullet} q(\mathbf{u})$ follows trivially. If $\|\mathfrak{h}_2\| > 0$, then there exists a rule

$$(\delta * p(\mathbf{x})) \mathrel{-\!\!\bullet} q(\mathbf{y}) \Leftarrow_{\mathfrak{C}_\mathcal{S}} \rho \tag{13}$$

and a substitution τ such that $[(\delta * p(\mathbf{x})) \mathrel{-\!\!\bullet} q(\mathbf{y})]\tau = (\beta * p(\mathbf{t})) \mathrel{-\!\!\bullet} q(\mathbf{u})$ and $(\mathfrak{s}', \mathfrak{h}_2) \models \rho\tau$, where $\mathfrak{s}'$ is an associate of $\mathfrak{s}$. Since $\|\mathfrak{h}_2\| > 0$, by definition of $\mathfrak{C}_\mathcal{S}$, rule (13) must be an instance of (II). Thus ρ is of the form $\exists \mathbf{v} \,.\, \psi'\sigma * \circledast_{j=1}^{m} (\gamma_j \mathrel{-\!\!\bullet} p_j(\sigma(\mathbf{w}_j)))$ for some substitution σ, where $\gamma_1, \ldots, \gamma_m$ are separating conjunctions of predicate atoms such that $\delta * p(\mathbf{x}) = \circledast_{j=1}^{m} \gamma_j$. Still because (13) is an instance of (II), there exists a rule

$$q(\mathbf{y}) \Leftarrow_\mathcal{S} \exists \mathbf{z} \,.\, \psi' * \circledast_{j=1}^{m} p_j(\mathbf{w}_j) \tag{14}$$

and we have $\mathbf{v} = \mathbf{z} \setminus \mathrm{dom}(\sigma)$.

Since $(\mathfrak{s}, \mathfrak{h}_2) \models_{\mathfrak{C}_\mathcal{S}} \exists \mathbf{v} \,.\, \psi'\sigma\tau * \circledast_{j=1}^{m} \gamma_j\tau \mathrel{-\!\!\bullet} p_j(\tau(\sigma(\mathbf{w}_j)))$, there exists a $\mathbf{v}$-associate $\overline{\mathfrak{s}}$ of $\mathfrak{s}$ such that $(\overline{\mathfrak{s}}, \mathfrak{h}_2) \models_{\mathfrak{C}_\mathcal{S}} \psi'\sigma\tau * \circledast_{j=1}^{m} \gamma_j\tau \mathrel{-\!\!\bullet} p_j(\tau(\sigma(\mathbf{w}_j)))$. Hence, there exist two disjoint heaps $\mathfrak{h}_2'$ and $\mathfrak{h}_2''$ such that $\mathfrak{h}_2 = \mathfrak{h}_2' \uplus \mathfrak{h}_2''$, $(\overline{\mathfrak{s}}, \mathfrak{h}_2') \models \psi'\sigma\tau$ and $(\overline{\mathfrak{s}}, \mathfrak{h}_2'') \models_{\mathfrak{C}_\mathcal{S}} \circledast_{j=1}^{m} \gamma_j\tau \mathrel{-\!\!\bullet} p_j(\tau(\sigma(\mathbf{w}_j)))$. We deduce that

$$(\overline{\mathfrak{s}}, \mathfrak{h}_1 \uplus \mathfrak{h}_2'') \models_{\mathfrak{C}_\mathcal{S}} [\alpha \mathrel{-\!\!\bullet} p(\mathbf{t})] * [\circledast_{j=1}^{m} \gamma_j\tau \mathrel{-\!\!\bullet} p_j(\tau(\sigma(\mathbf{w}_j)))].$$

Since $\delta * p(\mathbf{x}) = \circledast_{j=1}^{m} \gamma_j$, we can assume w.l.o.g. that γ_1 is of the form $p(\mathbf{x}) * \delta'$, so that $\gamma_1\tau = p(\mathbf{t}) * \delta'\tau$ and

$$(\overline{\mathfrak{s}}, \mathfrak{h}_1 \uplus \mathfrak{h}_2'') \models_{\mathfrak{C}_\mathcal{S}} [\alpha \mathrel{-\!\!\bullet} p(\mathbf{t})] * [p(\mathbf{t}) * \delta'\tau \mathrel{-\!\!\bullet} p_1(\tau(\sigma(\mathbf{w}_1)))] * [\circledast_{j=2}^{m} \gamma_j\tau \mathrel{-\!\!\bullet} p_j(\tau(\sigma(\mathbf{z}_j)))].$$

There therefore exist two disjoint heaps $\mathfrak{h}_3$ and $\mathfrak{h}_4$ such that $\mathfrak{h}_1 \uplus \mathfrak{h}_2'' = \mathfrak{h}_3 \uplus \mathfrak{h}_4$ and the following hold:

$$\begin{array}{lll} (\overline{\mathfrak{s}}, \mathfrak{h}_3) & \models_{\mathfrak{C}_\mathcal{S}} & [\alpha \mathrel{-\!\!\bullet} p(\mathbf{t})] * [p(\mathbf{t}) * \delta'\tau \mathrel{-\!\!\bullet} p_1(\tau(\sigma(\mathbf{z}_1)))], \\ (\overline{\mathfrak{s}}, \mathfrak{h}_4) & \models_{\mathfrak{C}_\mathcal{S}} & \circledast_{j=2}^{m} \gamma_j\tau \mathrel{-\!\!\bullet} p_j(\tau(\sigma(\mathbf{w}_j))). \end{array}$$

Because $\mathcal{S}$ is assumed to be progressing, ψ' contains exactly one points-to atom, thus $\|\mathfrak{h}_2'\| = 1$ and $\|\mathfrak{h}_3\| \leq \|\mathfrak{h}_1\| + \|\mathfrak{h}_2''\| < \|\mathfrak{h}_1\| + \|\mathfrak{h}_2\| = \|\mathfrak{h}\|$. By the inductive hypothesis, we deduce that $(\overline{\mathfrak{s}}, \mathfrak{h}_3) \models_{\mathfrak{C}_\mathcal{S}} \alpha * \delta'\tau \mathrel{-\!\!\bullet} p_1(\tau(\sigma(\mathbf{w}_1)))$. Putting it all together, we obtain

$$\begin{array}{lll} (\overline{\mathfrak{s}}, \mathfrak{h}) & \models_{\mathfrak{C}_\mathcal{S}} & \psi'\sigma\tau * [\alpha * \delta'\tau \mathrel{-\!\!\bullet} p_1(\tau(\sigma(\mathbf{w}_1)))] * [\circledast_{j=2}^{m} \gamma_j\tau \mathrel{-\!\!\bullet} p_j(\tau(\sigma(\mathbf{w}_j)))], \text{ hence} \\ (\mathfrak{s}, \mathfrak{h}) & \models_{\mathfrak{C}_\mathcal{S}} & \exists \mathbf{v} \,.\, \psi'\sigma\tau * [\alpha * \delta'\tau \mathrel{-\!\!\bullet} p_1(\tau(\sigma(\mathbf{w}_1)))] * [\circledast_{j=2}^{m} \gamma_j\tau \mathrel{-\!\!\bullet} p_j(\tau(\sigma(\mathbf{w}_j)))]. \end{array}$$

Since $\delta = \delta' * \circledast_{j=2}^{m} \gamma_j$, rule (14) implies the existence of the following rule that is an instance of (II):

$$(\eta * \delta) \multimap q(\mathbf{y}) \Leftarrow_{\mathfrak{C}_S} \exists \mathbf{v} \,.\, \psi'\sigma * [\eta * \delta' \multimap p_1(\sigma(\mathbf{w}_1))] * [\circledast_{j=2}^{m} \gamma_j \multimap p_j(\sigma(\mathbf{w}_j))],$$

where η is a separating conjunction of predicate atoms, such that $\eta\tau = \alpha$. Thus we obtain $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_S} (\eta\tau * \delta\tau) \multimap q(\tau(\mathbf{y}))$ and $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_S} \alpha * \beta \multimap q(\mathbf{u})$ follows. ◀

L Proof of Lemma 30 (Section 6)

"$\subseteq$" Let $\psi \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h})$ be a core formula. By equation (6), it is sufficient to show the existence of core formulæ $\psi_i \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}_i)$, for $i = 1, 2$, such that $\psi_1 * \psi_2 \Vdash_D \psi$.

(**A**) First, we proceed under the following assumptions:

1. ψ is quantifier-free thus, by Definition 19, it is of the form:

$$\psi = \circledast_{i=1}^{n} \underbrace{\left(\circledast_{j=1}^{k_i} q_j^i(\mathbf{u}_j^i) \multimap p_i(\mathbf{t}_i)\right)}_{\stackrel{\text{def}}{=} \lambda_{i \in [\![1..n]\!]}} * \circledast_{i=n+1}^{m} \underbrace{x_i \mapsto (t_1^i, \ldots, t_{\aleph}^i)}_{\stackrel{\text{def}}{=} \lambda_{i \in [\![n+1..m]\!]}}, \text{ for some } 0 \leq n \leq m,$$

2. $\dot{\mathfrak{s}}$ is bijective, i.e. $\mathrm{rng}(\dot{\mathfrak{s}}) = \mathbb{L}$;
3. $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_S} \psi$ and $\dot{\mathfrak{s}}(\mathrm{roots}_{\mathsf{lhs}}(\psi)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$ (†)

We show the existence of two quantifier-free core formulæ ψ_1, ψ_2 with $\psi_1, \psi_2 \Vdash_D \psi$, $\dot{\mathfrak{s}} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}, \mathfrak{h}_i, \psi_i)$ and $\mathrm{roots}(\psi_i) \subseteq \mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C} \cup \mathrm{roots}(\psi)$, for $i = 1, 2$. By definition, there exist m disjoint heaps $\mathfrak{h}'_1, \ldots, \mathfrak{h}'_m$, such that $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2 = \biguplus_{i=1}^{m} \mathfrak{h}'_i$ and $(\dot{\mathfrak{s}}, \mathfrak{h}'_i) \models_{\mathfrak{C}_S} \lambda_i$, for all $i \in [\![1 \,..\, m]\!]$. First, we prove that:

$$\mathrm{roots}_{\mathsf{lhs}}(\psi) \cap D = \emptyset. \quad (\dagger\dagger)$$

Suppose, for a contradiction, that there exists a variable $x \in \mathrm{roots}_{\mathsf{lhs}}(\psi) \cap D$. Then $\dot{\mathfrak{s}}(x) \in \dot{\mathfrak{s}}(\mathrm{roots}_{\mathsf{lhs}}(\psi))$, leading to $\dot{\mathfrak{s}}(x) \notin \mathrm{dom}(\mathfrak{h})$, by (†). But we also have $\dot{\mathfrak{s}}(x) \in \dot{\mathfrak{s}}(D)$, hence $\dot{\mathfrak{s}}(D) \not\subseteq \mathrm{dom}(\mathfrak{h})$, which contradicts the hypothesis $\dot{\mathfrak{s}}(D) \subseteq \dot{\mathfrak{s}}(\mathrm{dom}(\mathfrak{h})$ from the statement of the Lemma. Second, we build ψ_1 and ψ_2, distinguishing the following cases:

(**A.1**) If for all $i \in [\![1 \,..\, m]\!]$, either $\mathfrak{h}'_i \subseteq \mathfrak{h}_1$ or $\mathfrak{h}'_i \subseteq \mathfrak{h}_2$, then we let $\psi_i \stackrel{\text{def}}{=} \circledast\{\lambda_j \mid j \in [\![1 \,..\, m]\!],\ \mathfrak{h}'_j \subseteq \mathfrak{h}_i\}$, for $i = 1, 2$ (note that we may have $\psi_i = \mathsf{emp}$, if $\mathfrak{h}_i$ is empty). It is clear that the formula ψ can be written in the form $\psi_1 * \psi_2$, up the commutativity of $*$ and neutrality of emp for $*$. Since $\mathrm{roots}_{\mathsf{lhs}}(\psi) \cap D = \emptyset$ by (††), we deduce that $\psi_1, \psi_2 \Vdash_D \psi$ (5) trivially, since $\psi = \psi_1 * \psi_2$.

(**A.2**) Otherwise, there exists $i \in [\![1 \,..\, m]\!]$ such that $\mathfrak{h}'_i \not\subseteq \mathfrak{h}_1$ and $\mathfrak{h}'_i \not\subseteq \mathfrak{h}_2$. Thus, necessarily, $\|\mathfrak{h}'_i\| > 1$. Furthermore, since $\|\mathfrak{h}'_j\| = 1$ for all $j \in [\![n+1 \,..\, m]\!]$, we must have $i \in [\![1 \,..\, n]\!]$. For the sake of readability we drop all references to i and write $\lambda_i = \circledast_{j=1}^{k} q_j(\mathbf{u}_j) \multimap p(\mathbf{t})$ instead of $\lambda_i = \circledast_{j=1}^{k_i} q_j^i(\mathbf{u}_j^i) \multimap p_i(\mathbf{t}_i)$. Since $\dot{\mathfrak{s}}$ is bijective by assumption, by Lemma 49, there exists a core unfolding $\lambda_i \rightsquigarrow_{\mathfrak{C}_S} \varphi_i$, such that $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_S} \varphi_i$. Because $\|\mathfrak{h}'_i\| > 1$, entails that $\varphi_i \neq \mathsf{emp}$, the rule used to obtain this core unfolding (see Definition 21) must have been generated by inference rule (II). Since $\mathcal{S}$ is progressing, we deduce that φ_i is of the form $t_0 \mapsto (t_1, \ldots, t_{\aleph}) * \circledast_{j=1}^{k'} (\gamma_j \multimap p'_j(\mathbf{t}_j))$, for some separating conjunctions of predicate atoms $\gamma_1, \ldots, \gamma_{k'}$ such that $\circledast_{j=1}^{k'} \gamma_j = \circledast_{j=1}^{k} q_j(\mathbf{u}_j)$, and that $t_0 = \mathsf{root}(p(\mathbf{t}))$. Then $\dot{\mathfrak{s}}(t_0) \in \mathrm{dom}(\mathfrak{h}'_i) \subseteq \mathrm{dom}(\mathfrak{h})$ and assume that $\dot{\mathfrak{s}}(t_0) \in \mathrm{dom}(\mathfrak{h}_1)$ (the case $\dot{\mathfrak{s}}(t_0) \in \mathrm{dom}(\mathfrak{h}_2)$ is symmetric). We construct a sequence of formulæ by applying the same process to each occurrence of a subformula of the form $\alpha' \multimap p'(\mathbf{t}')$ such that $\dot{\mathfrak{s}}(\mathsf{root}(p'(\mathbf{t}'))) \in \mathrm{dom}(\mathfrak{h}_1)$, leading to $\circledast_{j=1}^{k} q_j(\mathbf{u}_j) \multimap p(\mathbf{t}) \rightsquigarrow^*_{\mathfrak{C}_S} \alpha * \circledast_{j=1}^{h} \delta_j \multimap r_j(\mathbf{v}_j)$, where:

- α is a separating conjunction of points-to atoms,
- $\delta_1, \ldots, \delta_h$ are separating conjunctions of predicate atoms, such that $\circledast_{j=1}^{h} \delta_j = \circledast_{j=1}^{k} q_j(\mathbf{u}_j)$,
- $(\dot{\mathfrak{s}}, \mathfrak{h}'_i) \models_{\mathfrak{C}_S} \alpha * \circledast_{j=1}^{h} \delta_j \multimap r_j(\mathbf{v}_j)$,
- $\dot{\mathfrak{s}}(\mathsf{root}(r_j(\mathbf{v}_j))) \in \mathrm{dom}(\mathfrak{h}_2)$, for all $j \in [\![1 \,..\, h]\!]$.

Let $\lambda^1_{i,1} \stackrel{\text{def}}{=} \mathbin{\ast}^h_{j=1} r_j(\mathbf{v}_j) \mathrel{-\!\!\bullet} p(\mathbf{t})$. By definition $\mathfrak{h}'_i = \mathfrak{h}^1_{i,1} \uplus \mathfrak{h}'_{i,1}$, with $(\dot{\mathfrak{s}}, \mathfrak{h}^1_{i,1}) \models_{\mathfrak{C}_\mathcal{S}} \alpha$ and $(\dot{\mathfrak{s}}, \mathfrak{h}'_{i,1}) \models_{\mathfrak{C}_\mathcal{S}} \mathbin{\ast}^h_{j=1} \delta_j \mathrel{-\!\!\bullet} r_j(\mathbf{v}_j)$. Note that by construction $\mathfrak{h}^1_{i,1} \subseteq \mathfrak{h}^1$ (but we do not necessarily have $\mathfrak{h}'_{i,1} \subseteq \mathfrak{h}_2$). Furthermore, it is easy to check that $\alpha \models_{\mathfrak{C}_\mathcal{S}} \lambda^1_{i,1}$ (indeed, by construction, α is obtained by starting from $p(\mathbf{t})$ and repeatedly unfolding all atoms not occurring in $\mathbin{\ast}^h_{j=1} r_j(\mathbf{v}_j)$), hence $(\dot{\mathfrak{s}}, \mathfrak{h}^1_{i,1}) \models_{\mathfrak{C}_\mathcal{S}} \lambda^1_{i,1}$. By Definition 28, we have $\lambda^1_{i,1} \ast \left(\mathbin{\ast}^h_{j=1} \delta_j \mathrel{-\!\!\bullet} r_j(\mathbf{v}_j) \right) \Vdash^* \lambda_i$. We now prove that:

$$\mathsf{root}(r_j(\mathbf{v}_j)) \in \mathcal{V}^1_\mathcal{P} \cup \mathbb{C}, \text{ for each } j \in [\![1 \,..\, h]\!]. \quad (\star)$$

Since $(\dot{\mathfrak{s}}, \mathfrak{h}^1_{i,1}) \models_{\mathfrak{C}_\mathcal{S}} \lambda^1_{i,1}$, by Lemma 44, we have $\dot{\mathfrak{s}}(\mathsf{root}(r_j(\mathbf{v}_j))) \in \mathrm{loc}(\mathfrak{h}_1) \cup \dot{\mathfrak{s}}(\mathbb{C})$. If $\dot{\mathfrak{s}}(\mathsf{root}(r_j(\mathbf{v}_j))) \in \dot{\mathfrak{s}}(\mathbb{C})$, we obtain $\mathsf{root}(r_j(\mathbf{v}_j)) \in \mathbb{C}$ by injectivity of $\dot{\mathfrak{s}}$. Otherwise $\dot{\mathfrak{s}}(\mathsf{root}(r_j(\mathbf{v}_j))) \in \mathrm{loc}(\mathfrak{h}_1)$, and since $\dot{\mathfrak{s}}(\mathsf{root}(r_j(\mathbf{v}_j))) \in \mathrm{dom}(\mathfrak{h}_2) \subseteq \mathrm{loc}(\mathfrak{h}_2)$ by construction, we obtain $\dot{\mathfrak{s}}(\mathsf{root}(r_j(\mathbf{v}_j))) \in \mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \subseteq \dot{\mathfrak{s}}(\mathcal{V}^1_\mathcal{P} \cup \mathbb{C})$, by hypothesis (3) of the Lemma. Since $\dot{\mathfrak{s}}$ is injective, we deduce that $\mathsf{root}(r_j(\mathbf{v}_j)) \in \mathcal{V}^1_\mathcal{P} \cup \mathbb{C}$.

We repeat the entire process until we get a formula that satisfies Condition (**A.1**). Note that the unfolding terminates because at each step we increase the number h of separating conjunctions $\delta_1, \ldots, \delta_h$ and $\mathbin{\ast}^h_{j=1} \delta_j = \mathbin{\ast}^k_{j=1} q_j(\mathbf{u}_j)$, where $k \geq h$ is fixed. If we denote by s the number of unfolding steps, and by $\psi(i)$ the formula obtained after step i, we eventually obtain a sequence of formulæ $\psi(s) \Vdash^* \ldots \Vdash^* \psi(0) = \psi$ where $\psi(s)$ satisfies Condition (**A.1**), and $(\dot{\mathfrak{s}}, \mathfrak{h}) \models \psi(i)$, for all $i = 0, \ldots, s$. By Point (**A.1**), we therefore obtain formulæ ψ_j such that $(\dot{\mathfrak{s}}, \mathfrak{h}_j) \models_{\mathfrak{C}_\mathcal{S}} \psi_j$, for $j = 1, 2$ and $\psi_1 \ast \psi_2 \Vdash^* \psi$, which, by (††), leads to $\psi_1, \psi_2 \Vdash_D \psi$ (5).

We prove that $\dot{\mathfrak{s}}(\mathrm{roots}_{\mathsf{lhs}}(\psi_i)) \cap \mathrm{dom}(\mathfrak{h}_i) = \emptyset$, for $i = 1, 2$. Let $i = 1$ and $x \in \mathrm{roots}_{\mathsf{lhs}}(\psi_1)$ (the proof is identical for the case $i = 2$). If $x \in \mathrm{roots}_{\mathsf{lhs}}(\psi)$ then $\dot{\mathfrak{s}}(x) \notin \mathrm{dom}(\mathfrak{h})$, by (†). Otherwise, $x \notin \mathrm{roots}_{\mathsf{lhs}}(\psi)$ was introduced during the unfolding, hence $\dot{\mathfrak{s}}(x) \in \mathrm{dom}(\mathfrak{h}_2)$, by the construction of ψ_1. In both cases, we have $\dot{\mathfrak{s}}(x) \notin \mathrm{dom}(\mathfrak{h}_1)$. Since $(\dot{\mathfrak{s}}, \mathfrak{h}_1) \models_{\mathfrak{C}_\mathcal{S}} \psi_1$ and ψ_1 is quantifier-free, by construction, we have $\dot{\mathfrak{s}} \in \mathcal{W}_\mathcal{S}(\dot{\mathfrak{s}}, \mathfrak{h}_1, \psi_1)$, thus $\psi_1 \in C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h}_1)$, as required.

Next, we show that for $i = 1, 2$, each root in ψ_i is contained in $\mathcal{V}^1_\mathcal{P} \cup \mathbb{C} \cup \mathrm{roots}(\psi)$, and that it occurs with multiplicity one. We give the proof when $i = 1$, the proof for $i = 2$ is symmetric. First, each $x \in \mathrm{roots}(\psi_1)$ is either a root of ψ or it is introduced by the unfoldings described above. In the second case we have $x \in \mathcal{V}^1_\mathcal{P} \cup \mathbb{C}$ by ($\star$). Second, we show that all variables from $\mathrm{roots}(\psi_1)$ occur with multiplicity one. Suppose, for a contradiction, that x occurs twice as a root in ψ_1. If both occurrences of x are in points-to atoms $x \mapsto (t_1, \ldots, t_\aleph)$ or in a predicate atom $\delta \mathrel{-\!\!\bullet} p(\mathbf{t})$ with $x = \mathsf{root}(p(\mathbf{t}))$, then since all atoms are conjoined by separating conjunctions, ϕ_1 is unsatisfiable, which contradicts the fact that $(\dot{\mathfrak{s}}, \mathfrak{h}_1) \models_{\mathfrak{C}_\mathcal{S}} \psi_1$. If one occurrence of x occurs in $\mathrm{roots}_{\mathsf{lhs}}(\psi_1)$ then we have shown that $\dot{\mathfrak{s}}(x) \notin \mathrm{dom}(\mathfrak{h}_1)$, thus the other occurrence of x cannot occur in $\mathrm{roots}_{\mathsf{rhs}}(\psi_1)$, which entails that it also occurs in $\mathrm{roots}_{\mathsf{lhs}}(\psi_1)$. Finally, assume that both occurrences of x occur in $\mathrm{roots}_{\mathsf{lhs}}(\psi_1)$. Because $\psi \in \mathsf{Core}(\mathcal{P})$, it must be the case that at least one occurrence of x was introduced during the unfolding. This entails that $\dot{\mathfrak{s}}(x) \in \mathrm{dom}(\mathfrak{h})$ thus x cannot occur in $\mathrm{roots}_{\mathsf{lhs}}(\psi)$, because $\psi \in C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h})$ (Definition 23), hence both occurrences of x have been introduced during the unfolding. But each time a variable x is introduced in $\mathrm{roots}_{\mathsf{lhs}}(\psi_1)$, there is another occurrence of the same variable x that is introduced in $\mathrm{roots}_{\mathsf{rhs}}(\psi_2)$, hence ψ_2 is unsatisfiable, which contradicts the fact that $(\dot{\mathfrak{s}}, \mathfrak{h}_2) \models_{\mathfrak{C}_\mathcal{S}} \psi_2$.

(**B**) Let $\psi = \exists_\mathsf{h} \mathbf{x} \forall_{\neg \mathsf{h}} \mathbf{y} \,.\, \varphi$, where φ is a quantifier-free core formula in $\mathsf{Core}(\mathcal{P})$ and let $\dot{\mathfrak{s}}$ be an injective store. Note that, since $\psi \in \mathsf{Core}(\mathcal{P})$ and $\mathrm{dom}(\dot{\mathfrak{s}}) \subseteq \mathcal{V}^1_\mathcal{P}$, we have $(\mathbf{x} \cup \mathbf{y}) \cap \mathrm{dom}(\dot{\mathfrak{s}}) = \emptyset$. Because $\psi \in C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h})$, by Definition 23, there exists a witness $\dot{\bar{\mathfrak{s}}} \in \mathcal{W}_\mathcal{S}(\dot{\mathfrak{s}}, \mathfrak{h}, \psi)$, satisfying the three points of Definition 23, and such that:

$$\dot{\bar{\mathfrak{s}}}(\mathrm{roots}_{\mathsf{lhs}}(\psi)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset. \quad (\ddagger)$$

Note that $\dot{\bar{\mathfrak{s}}}$ is injective by Definition 23, and we can assume w.l.o.g. that it is bijective.

To this aim, we consider any bijection $\ell \mapsto x_\ell$ between $\mathbb{L} \setminus \mathrm{rng}(\dot{\bar{\mathfrak{s}}})$ and $\mathbb{V} \setminus \mathrm{dom}(\dot{\bar{\mathfrak{s}}})$. Such a bijection

exists because both $\mathbb{L} \setminus \mathrm{rng}(\dot{\mathfrak{s}})$ and $\mathbb{V} \setminus \mathrm{dom}(\dot{\mathfrak{s}})$ are infinitely countable. Let $\dot{\mathfrak{s}}'$ be the extension of $\dot{\mathfrak{s}}$ with the set of pairs $\{(x_\ell, \ell) \mid \ell \mapsto x_\ell\}$. It is easy to check that $\dot{\mathfrak{s}}'$ is bijective.

Since $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_\mathcal{S}} \varphi$ by point 1 of Definition 23 and φ is quantifier-free, we have $\dot{\mathfrak{s}} \in \mathcal{W}_\mathcal{S}(\dot{\mathfrak{s}}, \mathfrak{h}, \varphi)$, hence $\varphi \in C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h})$, because $\mathrm{roots}_{\mathsf{lhs}}(\varphi) = \mathrm{roots}_{\mathsf{lhs}}(\psi)$ and $\dot{\mathfrak{s}}(\mathrm{roots}_{\mathsf{lhs}}(\varphi)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$ follows from (‡). By case (**A**), there exist quantifier-free core formulæ φ_1, φ_2, such that $\varphi_1, \varphi_2 \Vdash_D \varphi$, $\dot{\mathfrak{s}} \in \mathcal{W}_\mathcal{S}(\dot{\mathfrak{s}}, \mathfrak{h}_i, \varphi_i)$ and $\mathrm{roots}(\varphi_i) \subseteq \mathcal{V}^1_\mathcal{P} \cup \mathbb{C} \cup \mathrm{roots}(\varphi)$, for $i = 1, 2$. Let $\dot{\mathfrak{s}}_i$ be the restriction of $\dot{\mathfrak{s}}$ to $\mathsf{fv}(\varphi_i) \cup \mathbb{C}$ and define the following sets, for $i = 1, 2$:

$$\mathbf{x}_i \stackrel{\text{def}}{=} \left\{ x \in \mathrm{dom}(\dot{\mathfrak{s}}) \setminus \mathrm{dom}(\dot{\mathfrak{s}}_i) \mid \dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}_i) \right\} \qquad \mathbf{y}_i \stackrel{\text{def}}{=} \left\{ x \in \mathrm{dom}(\dot{\mathfrak{s}}_i) \setminus \mathrm{dom}(\dot{\mathfrak{s}}) \mid \dot{\mathfrak{s}}(x) \notin \mathrm{loc}(\mathfrak{h}_i) \right\}$$

Note that we do not know at this point whether $\mathbf{x}_i \subseteq \mathrm{dom}(\dot{\mathfrak{s}}_i)$ (this will be established later), while $\mathbf{y}_i \subseteq \mathrm{dom}(\dot{\mathfrak{s}}_i)$ holds by definition.

We prove that for all variables $x \in \mathbf{x}_i$, there exists a subformula δ occurring in φ_i such that $x \in \mathsf{fv}(\delta)$, and either δ is a points-to atom or $\delta = \alpha \mathrel{-\!\!\bullet} \beta$ with $x \in \mathsf{fv}(\beta) \setminus \mathsf{fv}(\alpha)$. To this aim, we begin by proving that if some formula φ' is obtained from the initial formula φ by a sequence of unfoldings as defined in Part (**A**) and if $x \in \mathsf{fv}(\varphi')$, then φ' contains a formula of the form above. The proof is by induction on the length of the unfolding:

- If $\varphi = \varphi'$, then by the hypothesis $x \notin \mathrm{dom}(\dot{\mathfrak{s}})$ and $x \in \mathsf{fv}(\varphi)$, thus $x \in \mathbf{x} \cup \mathbf{y}$. Since $\dot{\mathfrak{s}}_i(x) \in \mathrm{loc}(\mathfrak{h}_i) \subseteq \mathrm{loc}(\mathfrak{h})$, we have $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h})$, hence by Condition (3) of Definition 23, necessarily $x \in \mathbf{x}$. Then the proof follows immediately from Condition (ii) in Definition 19.
- Otherwise, according to the construction above, φ' is obtained from an unfolding φ'' of φ, by replacing some formula $\lambda_i = \mathbin{\raisebox{0.5ex}{$\scriptstyle *$}}_{j=1}^{k_i} q^i_j(\mathbf{u}^i_j) \mathrel{-\!\!\bullet} p_i(\mathbf{t}_i)$ in φ'' by $\lambda^1_{i,1} * \left(\mathbin{\raisebox{0.5ex}{$\scriptstyle *$}}_{j=1}^{h} (\delta_j \mathrel{-\!\!\bullet} r_j(\mathbf{v}_j)) \right)$, with $\lambda^1_{i,1} = \mathbin{\raisebox{0.5ex}{$\scriptstyle *$}}_{j=1}^{h} \left(r_j(\mathbf{v}_j) \mathrel{-\!\!\bullet} p_i(\mathbf{t}_i) \right)$, and all atoms in δ_j occur in $\mathbin{\raisebox{0.5ex}{$\scriptstyle *$}}_{j=1}^{k_i} q^i_j(\mathbf{u}^i_j)$.
  - If x occurs in φ'', then by the induction hypothesis φ'' contains a formula δ satisfying the condition above. If δ is distinct from λ_i then δ occurs in φ' and the proof is completed. Otherwise, we have $\delta = \alpha \mathrel{-\!\!\bullet} \beta$ with $\beta = p_i(\mathbf{t}_i)$, $\alpha = \mathbin{\raisebox{0.5ex}{$\scriptstyle *$}}_{j=1}^{k_i} q^i_j(\mathbf{u}^i_j)$ and $x \in \mathsf{fv}(\beta) \setminus \mathsf{fv}(\alpha)$. We distinguish two cases: If $x \in \mathsf{fv}(r_j(\mathbf{v}_j))$, for some $j \in [\![1 \,..\, h]\!]$, then $x \in \mathsf{fv}(r_j(\mathbf{v}_j)) \setminus \mathsf{fv}(\delta_j)$ (since $x \notin \mathsf{fv}(\alpha)$ and $\mathsf{fv}(\delta_j) \subseteq \mathsf{fv}(\alpha)$), thus the formula $\mathbin{\raisebox{0.5ex}{$\scriptstyle *$}}_{j=1}^{h} \delta_j \mathrel{-\!\!\bullet} r_j(\mathbf{v}_j)$ fulfills the required property. Otherwise, $x \in \mathsf{fv}(p_i(\mathbf{t}_i)) \setminus \mathsf{fv}(\mathbin{\raisebox{0.5ex}{$\scriptstyle *$}}_{j=1}^{h} r_j(\mathbf{v}_j))$ and $\lambda^1_{i,1}$ fulfills the property.
  - Now assume that x does not occur in φ''. This necessarily entails that $x \in \mathsf{fv}(r_j(\mathbf{v}_j))$, for some $j \in [\![1 \,..\, h]\!]$, and that $x \notin \mathsf{fv}(\delta_j)$, thus $x \in \mathsf{fv}(r_j(\mathbf{v}_j)) \setminus \mathsf{fv}(\delta_j)$ and the formula $\delta_j \mathrel{-\!\!\bullet} r_j(\mathbf{v}_j)$ fulfills the required property.

We show that such a formula δ cannot occur in φ_{3-i}, hence necessarily occurs in φ_i, which entails that $x \in \mathrm{dom}(\dot{\mathfrak{s}}_i)$, and also that $\mathbf{x}_1 \cap \mathbf{x}_2 = \emptyset$. This is the case because if δ occurs in φ_{3-i}, then there exists a subheap $\mathfrak{h}'_{3-i}$ of $\mathfrak{h}_{3-i}$ such that $(\dot{\mathfrak{s}}, \mathfrak{h}'_{3-i}) \models \delta$. By Lemma 45, since $x \in \mathsf{fv}(\beta) \setminus \mathsf{fv}(\alpha)$ when δ is of the form $\alpha \mathrel{-\!\!\bullet} \beta$, we have $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}_{3-i})$. Furthermore, by hypothesis $x \in \mathbf{x}_i$, hence $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}_i)$. Therefore $\dot{\mathfrak{s}}(x) \in \mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \subseteq \mathrm{rng}(\dot{\mathfrak{s}})$ by the hypothesis (2) of the Lemma. Since $\dot{\mathfrak{s}}$ is injective, this entails that $x \in \mathrm{dom}(\dot{\mathfrak{s}})$, which contradicts the definition of $\mathbf{x}_i$.

Let $\psi_i \stackrel{\text{def}}{=} \exists_\mathsf{h} \mathbf{x}_i \exists_\mathsf{h} \mathbf{y}_i \,.\, \varphi_i$, for $i = 1, 2$. Due to the previous property, ψ_i satisfies Condition (ii) of Definition 19. By definition of $\mathbf{y}_i$, we have $\mathbf{y}_i \subseteq \mathrm{dom}(\mathfrak{s}_i)$ and by definition of $\mathfrak{s}_i$, we have $\mathrm{dom}(\mathfrak{s}_i) \subseteq \mathsf{fv}(\varphi_i) \cup \mathbb{C}$, thus ψ_i also fulfills Condition (i) of the same definition. By part (**A**) φ_i is a core formula, hence Condition (iii) is satisfied, which entails that ψ_i is a core formula. Still by part (**A**) of the proof, $(\dot{\mathfrak{s}}, \mathfrak{h}_i) \models_{\mathfrak{C}_\mathcal{S}} \varphi_i$, thus we also have also $(\dot{\mathfrak{s}}_i, \mathfrak{h}_i) \models_{\mathfrak{C}_\mathcal{S}} \varphi_i$, by the definition of $\dot{\mathfrak{s}}_i$, for $i = 1, 2$. By the definition of $\mathbf{x}_i$ and $\mathbf{y}_i$, we have $\dot{\mathfrak{s}}_i \in \mathcal{W}_\mathcal{S}(\dot{\mathfrak{s}}, \mathfrak{h}_i, \psi_i)$ and since $\dot{\mathfrak{s}}_i(\mathrm{roots}_{\mathsf{lhs}}(\varphi_i)) = \dot{\mathfrak{s}}(\mathrm{roots}_{\mathsf{lhs}}(\varphi_i))$ and $\dot{\mathfrak{s}}(\mathrm{roots}_{\mathsf{lhs}}(\varphi_i)) \cap \mathrm{dom}(\mathfrak{h}_i) = \emptyset$, we obtain $\psi_i \in C_\mathcal{P}(\dot{\mathfrak{s}}, \mathfrak{h}_i)$, for $i = 1, 2$.

Since $\varphi_1 * \varphi_2 \Vdash_D \varphi$ and φ_1, φ_2 are quantifier-free, we have, by definition of $\Vdash_D$:

$$\psi_1 * \psi_2 \Vdash_D \exists_\mathsf{h} \mathbf{x}' \forall_{\neg \mathsf{h}} \mathbf{y}' \varphi, \text{ where } \mathbf{x}' = (\mathbf{x}_1 \cup \mathbf{x}_2) \cap \mathsf{fv}(\varphi) \text{ and } \mathbf{y}' = ((\mathbf{y}_1 \cup \mathbf{y}_2) \cap \mathsf{fv}(\varphi)) \setminus \mathbf{x}'.$$

To complete the proof, it is sufficient to show that $\mathbf{x}' = \mathbf{x}$ and that $\mathbf{y} = \mathbf{y}'$, so that $\exists_{\mathsf{h}}\mathbf{x}'\forall_{\neg\mathsf{h}}\mathbf{y}'\varphi = \psi$.

$\mathbf{x}' = \mathbf{x}$ "$\subseteq$" Let $x \in \mathbf{x}'$. We have $x \in \mathbf{x}_i$, for some $i = 1,2$, and $x \in \mathsf{fv}(\varphi)$. By definition of $\mathbf{x}_i$, this entails that $x \in \mathrm{dom}(\dot{\mathfrak{s}}) \setminus \mathrm{dom}(\dot{\mathfrak{s}})$ and that $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}_i) \subseteq \mathrm{loc}(\mathfrak{h})$. Since $x \in \mathsf{fv}(\varphi)$ and $x \in \mathrm{dom}(\dot{\mathfrak{s}}) \setminus \mathrm{dom}(\dot{\mathfrak{s}})$, necessarily $x \in \mathbf{x} \cup \mathbf{y}$, and because of Condition (3) in Definition 23, we have $x \notin \mathbf{y}$. Hence $x \in \mathbf{x}$.
"$\supseteq$" Let $x \in \mathbf{x}$. We have $x \in \mathsf{fv}(\varphi)$ by Definition 19 (ii), and $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h})$ by Definition 23 (1), thus $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}_i)$, for some $i = 1,2$, so that $x \in \mathbf{x}_i$. Consequently $x \in \mathbf{x}'$.

$\mathbf{y} = \mathbf{y}'$ "$\subseteq$" Let $y \in \mathbf{y}'$. By definition, we have $y \in \mathbf{y}_i$ for some $i = 1,2$, $y \in \mathsf{fv}(\varphi)$, and $y \notin \mathbf{x} = \mathbf{x}'$. Since $y \in \mathbf{y}_i$, we have $y \notin \mathrm{dom}(\dot{\mathfrak{s}})$, thus $y \notin \mathsf{fv}(\psi)$, hence $y \in \mathbf{x} \cup \mathbf{y}$. Since $y \notin \mathbf{x}$, we deduce that $y \in \mathbf{y}$.
"$\supseteq$" Let $y \in \mathbf{y}$. By definition, $y \notin \mathrm{dom}(\dot{\mathfrak{s}})$ and $y \notin \mathbf{x}$, moreover $y \in \mathsf{fv}(\varphi)$, by Definition 19 (i). By Definition 23 (3), we have $\dot{\mathfrak{s}}(y) \notin \mathrm{loc}(\mathfrak{h})$. By definition of $\Vdash_D$, since $y \in \mathsf{fv}(\varphi)$, necessarily $y \in \mathsf{fv}(\varphi_i)$, for some $i = 1,2$. Since $y \notin \mathrm{dom}(\dot{\mathfrak{s}})$, we deduce that $y \in \mathbf{x}_i \cup \mathbf{y}_i$. Since $\dot{\mathfrak{s}}(y) \notin \mathrm{loc}(\mathfrak{h})$, we have $\dot{\mathfrak{s}}(y) \notin \mathrm{loc}(\mathfrak{h}_i)$, hence $y \in \mathbf{y}_i$. Consequently, $y \in \mathbf{y}'$.

"$\supseteq$" Let $\psi \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}_1) \circledast_D C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}_2)$ be a core formula. By the definition of $\circledast_D$ (6), there exists $\psi_i \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}_i)$, for $i = 1,2$, such that $\psi_1, \psi_2 \Vdash_D \psi$. By the definition of $\Vdash_D$ (5), we have $\psi_i = \exists_{\mathsf{h}}\mathbf{x}_i\forall_{\neg\mathsf{h}}\mathbf{y}_i \,.\, \phi_i$, for $i = 1,2$, with $\mathbf{x} = (\mathbf{x}_1 \cup \mathbf{x}_2) \cap \mathsf{fv}(\phi)$, $\mathbf{y} = ((\mathbf{y}_1 \cup \mathbf{y}_2) \cap \mathsf{fv}(\phi)) \setminus \mathbf{x}$, $\mathbf{x}_1 \cap \mathbf{x}_2 = \emptyset$ and $\psi = \exists_{\mathsf{h}}\mathbf{x}\forall_{\neg\mathsf{h}}\mathbf{y} \,.\, \phi$, where ϕ_1, ϕ_2 and ϕ are quantifier-free core formulæ and $\mathrm{roots}_{\mathsf{lhs}}(\phi) \cap D = \emptyset$. Since $\psi_i \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h}_i)$, by Definition 23, there exist witnesses $\dot{\mathfrak{s}}_i \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}, \mathfrak{h}_i, \forall_{\neg\mathsf{h}}\mathbf{y}_i \,.\, \phi_i)$, such that $\dot{\mathfrak{s}}_i(\mathbf{x}_i) \subseteq \mathrm{loc}(\mathfrak{h}_i)$ and $\dot{\mathfrak{s}}_i(\mathrm{roots}_{\mathsf{lhs}}(\phi_i)) \cap \mathrm{dom}(\mathfrak{h}_i) = \emptyset$, for $i = 1,2$. W.l.o.g. we can choose these witnesses such that $\mathrm{dom}(\dot{\mathfrak{s}}_i) = \mathbf{x}_i \cup \mathrm{dom}(\dot{\mathfrak{s}})$. Let $\dot{\mathfrak{s}}$ be any extension of $\dot{\mathfrak{s}}_1 \cup \dot{\mathfrak{s}}_2$ such that $\mathbf{y}_1 \cup \mathbf{y}_2 \subseteq \mathrm{dom}(\dot{\mathfrak{s}})$ and $\dot{\mathfrak{s}}(y_1) \neq \dot{\mathfrak{s}}(y_2) \notin \mathrm{loc}(\mathfrak{h}) \cup \mathrm{rng}(\dot{\mathfrak{s}}_1) \cup \mathrm{rng}(\dot{\mathfrak{s}}_2)$, for all variables $y_1 \neq y_2 \in \mathbf{y}_1 \cup \mathbf{y}_2$. Note that such an extension exists, because $\mathbb{L}$ is infinite and $\mathbf{y}_1$, $\mathbf{y}_2$ are finite. Moreover, $\dot{\mathfrak{s}}$ is a well-defined store, because $\dot{\mathfrak{s}}_1$ and $\dot{\mathfrak{s}}_2$ both agree over $\mathrm{dom}(\dot{\mathfrak{s}})$ and $\mathbf{x}_1 \cap \mathbf{x}_2 = \emptyset$.

We prove that $\dot{\mathfrak{s}}$ is injective. Suppose, for a contradiction, that $\dot{\mathfrak{s}}(x_1) = \dot{\mathfrak{s}}(x_2)$, for some variables $x_1 \neq x_2 \in \mathrm{dom}(\dot{\mathfrak{s}})$. By the definition of $\dot{\mathfrak{s}}$, since $\dot{\mathfrak{s}}_1$ and $\dot{\mathfrak{s}}_2$ are injective, the only possibility is $x_i \in \mathrm{dom}(\dot{\mathfrak{s}}_i) \setminus \mathrm{dom}(\dot{\mathfrak{s}}_{3-i})$, for $i = 1,2$ (hence $x_i \notin \mathrm{dom}(\dot{\mathfrak{s}})$). Then $x_i \in \mathbf{x}_i$ must be the case, thus $\dot{\mathfrak{s}}_i(x_i) \in \mathrm{loc}(\mathfrak{h}_i)$, leading to $\dot{\mathfrak{s}}_1(x_1) \in \mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \subseteq \mathrm{rng}(\dot{\mathfrak{s}})$, by the hypothesis of the Lemma, hence $x_i \in \mathrm{dom}(\dot{\mathfrak{s}})$, by injectivity of $\dot{\mathfrak{s}}$, which yields a contradiction.

We prove next that $\dot{\mathfrak{s}} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}, \mathfrak{h}, \phi)$. Since $\dot{\mathfrak{s}}_i \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}, \mathfrak{h}_i, \forall_{\neg\mathsf{h}}\mathbf{y}_i \,.\, \phi_i)$, we have $(\dot{\mathfrak{s}}_i, \mathfrak{h}_i) \models_{\mathfrak{C}_{\mathcal{S}}} \forall_{\neg\mathsf{h}}\mathbf{y}_i \,.\, \phi_i$, for $i = 1,2$. We show that $\dot{\mathfrak{s}}(\mathbf{y}_i) \cap \mathrm{loc}(\mathfrak{h}_i) = \emptyset$ for $i = 1,2$. Suppose, for a contradiction, that $i = 1$ and $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}_1)$, for some $x \in \mathbf{y}_1$ (the proof when $i = 2$ is symmetric). By definition of $\dot{\mathfrak{s}}$, this is possible only if $x \in \mathbf{x}_2$, and this entails that $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}_2)$,thus $\dot{\mathfrak{s}}(x) \in \mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \subseteq \dot{\mathfrak{s}}(\mathcal{V}^1_{\mathcal{P}} \cup \mathbb{C})$, by the hypothesis of the Lemma. By the injectivity of store $\dot{\mathfrak{s}}$, this entails that $x \in \mathrm{dom}(\dot{\mathfrak{s}})$, which contradicts the fact that $x \in \mathbf{x}_2$ (since, by definition of $\mathbf{x}_2$, we have $\mathbf{x}_2 \cap \mathrm{dom}(\dot{\mathfrak{s}}) = \emptyset$). Then $\dot{\mathfrak{s}}(\mathbf{y}_i) \cap \mathrm{loc}(\mathfrak{h}_i) = \emptyset$, hence, $(\dot{\mathfrak{s}}, \mathfrak{h}_i) \models_{\mathfrak{C}_{\mathcal{S}}} \phi_i$, for $i = 1,2$. Then $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi_1 * \phi_2$, leading to $(\dot{\mathfrak{s}}, \mathfrak{h}) \models_{\mathfrak{C}_{\mathcal{S}}} \phi$, by Lemma 57, since $\phi_1 * \phi_2 \Vdash^* \phi$. Moreover, $\dot{\mathfrak{s}}(\mathbf{x}_1 \cup \mathbf{x}_2) = \dot{\mathfrak{s}}_1(\mathbf{x}_1) \cup \dot{\mathfrak{s}}_2(\mathbf{x}_2) \subseteq \mathrm{loc}(\mathfrak{h}_1) \cup \mathrm{loc}(\mathfrak{h}_2) = \mathrm{loc}(\mathfrak{h})$ and $\dot{\mathfrak{s}}(\mathbf{y}_i) \cap \mathrm{loc}(\mathfrak{h}) = \emptyset$, for $i = 1,2$, by the definition of $\dot{\mathfrak{s}}$. Then $\dot{\mathfrak{s}} \in \mathcal{W}_{\mathcal{S}}(\dot{\mathfrak{s}}, \mathfrak{h}, \phi)$, by Definition 23.

Finally, we prove that $\dot{\mathfrak{s}}(\mathrm{roots}_{\mathsf{lhs}}(\phi)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$. Suppose, for a contradiction, that there exists $x \in \mathrm{roots}_{\mathsf{lhs}}(\phi)$ such that $\dot{\mathfrak{s}}(x) \in \mathrm{dom}(\mathfrak{h})$. By Definition 28, we have $\mathrm{roots}_{\mathsf{lhs}}(\phi) \subseteq \mathrm{roots}_{\mathsf{lhs}}(\phi_1) \cup \mathrm{roots}_{\mathsf{lhs}}(\phi_2)$ and we assume that $x \in \mathrm{roots}_{\mathsf{lhs}}(\phi_1)$ (the case $x \in \mathrm{roots}_{\mathsf{lhs}}(\phi_2)$ is symmetrical). Since $(\dot{\mathfrak{s}}, \mathfrak{h}_1) \models_{\mathfrak{C}_{\mathcal{S}}} \phi_1$, we obtain $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}_1) \cup \dot{\mathfrak{s}}(\mathbb{C})$, by Lemma 44, and since $x \notin \mathbb{C}$ and $\dot{\mathfrak{s}}$ is injective, we obtain $\dot{\mathfrak{s}}(x) \in \mathrm{loc}(\mathfrak{h}_1)$. Moreover, we have $\dot{\mathfrak{s}}_1(x) \notin \mathrm{dom}(\mathfrak{h}_1)$, hence $\dot{\mathfrak{s}}_1(x) \in \mathrm{dom}(\mathfrak{h}_2) \subseteq \mathrm{loc}(\mathfrak{h}_2)$. Thus $\dot{\mathfrak{s}}(x) \in \mathrm{Fr}(\mathfrak{h}_1, \mathfrak{h}_2) \cap \mathrm{dom}(\mathfrak{h}) \subseteq \dot{\mathfrak{s}}(D)$, leading to $x \in D$, by the injectivity of $\dot{\mathfrak{s}}$. This contradicts the hypothesis $\mathrm{roots}_{\mathsf{lhs}}(\phi) \cap D = \emptyset$ (5). We obtain that $\dot{\mathfrak{s}}(\mathrm{roots}_{\mathsf{lhs}}(\phi)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$, thus $\phi \in C_{\mathcal{P}}(\dot{\mathfrak{s}}, \mathfrak{h})$. ◀

M Proof of Lemma 31 (Section 7)

Let $\phi \in \mathsf{Core}(\mathcal{P})$ be a core formula. Then ϕ can be viewed as a formula built over atoms of the form $p(\mathbf{t})$ and $t_0 \mapsto (t_1, \ldots, t_{\mathfrak{K}})$ using the connectives $*$, $-\!\!\bullet$ and the quantifiers $\exists_{\mathsf{h}}$ and $\forall_{\neg\mathsf{h}}$. By

Definition 19 (iii), ϕ contains at most $\|\mathcal{V}_\mathcal{P}\|$ occurrences of such atoms. Since, by points (i) and (ii) of Definition 19, all the variables in ϕ necessary occur in an atom, this entails that ϕ contains at most $\|\mathcal{V}_\mathcal{P}\| \times \alpha$ (bound or free) variables, where $\alpha = \max(\{\#p \mid p \in \mathbb{P}\} \cup \{\mathfrak{K}+1\})$ denotes the maximal arity of the relation symbols (including $\mapsto$) in ϕ. Since each atom is of size at most $\alpha+1$ and since there is at most one connective $*$ or $-\!\!\bullet$ for each atom, we deduce that $\text{size}(\phi) \leq 2 \times \|\mathcal{V}_\mathcal{P}\| \times \alpha + \|\mathcal{V}_\mathcal{P}\| \times (\alpha+2)$. By definition, we have $\alpha \leq \text{width}(\mathcal{P})$, and $\mathcal{V}_\mathcal{P}$ is chosen is such a way that $\|\mathcal{V}_\mathcal{P}\| = 2 \times \text{width}(\mathcal{P})$, thus $\text{size}(\phi) = O(\text{width}(\mathcal{P})^2)$. The symbols that may occur in the formula include the set of free and bound variables, the predicate symbols and the symbols $\mapsto$, $*$, $-\!\!\bullet$ $\forall_{\neg\mathsf{h}}$, $\exists_\mathsf{h}$, yielding at most $(\|\mathcal{V}_\mathcal{P}\| \times \alpha) + \text{size}(\mathcal{P}) + 5 \leq \text{width}(\mathcal{P})^2 + \text{size}(\mathcal{P}) + 5$ symbols. Thus there are at most $(\text{width}(\mathcal{P})^2 + \text{size}(\mathcal{P}) + 5)^{O(\text{width}(\mathcal{P})^2)} = 2^{O(\text{width}(\mathcal{P})^3 \times \log(\text{size}(\mathcal{P})))}$ core formulæ in $\mathsf{Core}(\mathcal{P})$. ◀