A Complete Axiomatisation for Quantifier-Free Separation Logic

Stéphane Demri, Etienne Lozes, Alessio Mansutti

A COMPLETE AXIOMATISATION FOR QUANTIFIER-FREE SEPARATION LOGIC

STÉPHANE DEMRI, ÉTIENNE LOZES, AND ALESSIO MANSUTTI

LSV, CNRS, ENS Paris-Saclay - 4, avenue des Sciences - 91190 Gif-sur-Yvette
e-mail address: demri@lsv.fr

I3S - Les Algorithmes - Bâtiment Euclide B - 2000, route des Lucioles - 06900 Sophia Antipolis
e-mail address: etienne.lozes@i3s.unice.fr

LSV, CNRS, ENS Paris-Saclay - 4, avenue des Sciences - 91190 Gif-sur-Yvette
e-mail address: mansutti@lsv.fr

Abstract. We present the first complete axiomatisation for quantifier-free separation logic. The logic is equipped with the standard concrete heaplet semantics and the proof system has no external feature such as nominals/labels. It is not possible to rely completely on proof systems for Boolean BI as the concrete semantics needs to be taken into account. Therefore, we present the first internal Hilbert-style axiomatisation for quantifier-free separation logic. The calculus is divided in three parts: the axiomatisation of core formulae where Boolean combinations of core formulae capture the expressivity of the whole logic, axioms and inference rules to simulate a bottom-up elimination of separating connectives, and finally structural axioms and inference rules from propositional calculus and Boolean BI with the magic wand.

1. Introduction

The virtue of axiomatising program logics. Designing a Hilbert-style axiomatisation for your favourite logic is usually quite challenging. This does not lead necessarily to optimal decision procedures, but the completeness proof usually provides essential insights to better understand the logic at hand. That is why many logics related to program verification have been axiomatised, often requiring non-trivial completeness proofs. By way of example, there are axiomatisations for the linear-time μ-calculus [Kai95, Dou17], the modal μ-calculus [Wal00] or for the alternating-time temporal logic ATL [GvD06], the full computation tree logic CTL* [Rey01], for probabilistic extensions of μ-calculus [LMX16] or for a coalgebraic generalisation [SV18]. Concerning the separation logics that extend Hoare-Floyd logic to verify programs with mutable data structures (see e.g. [OP99, Rey02, IO01, O'H12, PSO18]), a Hilbert-style axiomatisation of Boolean BI has been introduced in [GLW06], but remained at the abstract level of Boolean BI. More recently, HyBBI [BV14],

Key words and phrases: separation logic, internal calculus, adjunct/quantifier elimination.
* This is the long version of the first part of [DLM20].

Preprint submitted to
Logical Methods in Computer Science

a hybrid version of Boolean BI has been introduced in order to axiomatise various classes of abstract separation logics; HyBBI naturally considers classes of abstract models (typically preordered partial monoids) but it does not fit exactly the heaplet semantics of separation logics. Furthermore, the addition of nominals (in the sense of hybrid modal logics, see e.g. [ABM01]) extends substantially the object language. Other frameworks to axiomatise classes of abstract separation logics can be found in [DP18, Doc19] and in [HCGT18], respectively with labelled tableaux calculi and with sequent-style proof systems.

Our motivations. Since the birth of separation logics, there has been a lot of interest in the study of decidability and computational complexity issues, see e.g. [COY01, BDL09, BIP10, CHO$^+$11, DGLWM17, BK18, DLM18a, Man18, Man20], and comparatively less attention to the design of proof systems, and even less with the puristic approach that consists in discarding any external feature such as nominals or labels in the calculi. The well-known advantages of such an approach include an exhaustive understanding of the expressive power of the logic and discarding the use of any external artifact referring to semantical objects. For instance, a tableaux calculus with labels for quantifier-free separation logic is designed in [GM10], whereas Hilbert-style calculi for abstract separation logics with nominals are defined in [BV14]. Similarly, display calculi for bunched logics are provided in [Bro12] but such calculi extend Gentzen-style proof systems by allowing new structural connectives, which provides an elegant means to simulate labels. In this paper, we advocate a puristic approach and aim at designing a Hilbert-style proof system for quantifier-free separation logic $\mathsf{SL}(*, -\!\!*)$ (which includes the separating conjunction $*$ and implication $-\!\!*$, as well as all Boolean connectives) and more generally for other separation logics, while remaining within the very logical language (see the second part of [DLM20]).[1] Consequently, in this work, we only focus on axiomatising separation logics, and we have no claim for practical applications in the field of program verification with separation logics. Aiming at internal calculi is a non-trivial task as the general frameworks for abstract separation logics make use of labels, see e.g. [DP18, HCGT18]. We cannot rely on label-free calculi for BI, see e.g. [Pym02, GLW06], as separation logics are usually understood as Boolean BI interpreted on models of heap memory and therefore require calculi that cannot abstract as much as it is the case for Boolean BI. Finally, there are many translations from separation logics into logics or theories, see e.g. [CGH05, PWZ13, BDL12, RISK16]. However, completeness cannot in general be inherited by sublogics as the proof system should only use the sublogic and therefore the axiomatisation of sublogics may lead to different methods. A more detailed discussion about the related work can be found in Section 7.

Our contribution. We propose a modular axiomatisation of quantifier-free separation logic, starting with a complete axiomatisation of a Boolean algebra of core formulae, and incrementally adding support for the spatial connectives: the separating conjunction and the separating implication (a.k.a. the magic wand). The same approach could be followed for other fragments of separation logic, as we did in the conference version of this paper [DLM20] (see also a similar approach in [DFM19]). Thus, our approach can be considered with the broader perspective of a generic method for axiomatising separation logics. Let us be a bit more precise.

[1] We aim at defining *internal* calculi according to the terminology from the Workshop on External and Internal Calculi for Non-Classical Logics, FLOC'18, Oxford, `http://weic2018.loria.fr`.

In Section 3, we present the first Hilbert-style proof system for $\mathsf{SL}(*, -\!\!*)$ that uses axiom schemas and rules involving only formulae of this logic. We mainly introduce our approach and present the notations that are used throughout the paper. Each formula of $\mathsf{SL}(*, -\!\!*)$ is equivalent to a Boolean combination of *core formulae*: simple formulae of the logic expressing elementary properties about the models [Loz04b]. Though core formulae (also called *test formulae*) have been handy in several occasions for establishing complexity results for separation logics, see e.g. [BDL09, DLM18a, Man18, EIP19], in the paper, these formulae are instrumental for the axiomatisation. Indeed, the axiomatisation of $\mathsf{SL}(*, -\!\!*)$ is designed starting from an axiomatisation of Boolean combinations of core formulae (introduced in Section 4), and adding axioms and rules that allow to syntactically transform every formula of $\mathsf{SL}(*, -\!\!*)$ into such Boolean combinations. This transformation is introduced in Section 5 and in Section 6: the former section shows how to eliminate the separating conjunction $*$, whereas the latter one treat the separating implication $-\!\!*$. Schematically, for a valid formula φ, we conclude $\vdash \varphi$ from $\vdash \varphi'$ and $\vdash \varphi' \Leftrightarrow \varphi$, where φ' is a Boolean combination of core formulae. Our methodology leads to a calculus that is divided in three parts: (1) the axiomatisation of Boolean combinations of core formulae, (2) axioms and inference rules to simulate a bottom-up elimination of separating the separating conjunction, and (3) axioms and inference rules to simulate a bottom-up elimination of the magic wand. Such an approach that consists in first axiomatising a syntactic fragment of the whole logic (in our case, the core formulae), is best described in [Dou17] (see also [Wal00, vB11, WC13, Lüc18, DFM19]). Section 7 compares works from the literature with our contribution, either for separation logics (abstract versions, fragments, etc.) or for knowledge logics for which the axiomatisation has been performed by using a reduction to a strict syntactic fragment though expressively complete.

This paper is the complete version of the first part of [DLM20] dedicated to quantifier-free separation logic $\mathsf{SL}(*, -\!\!*)$. The complete version of the second part of [DLM20] dedicated to the new separation logic $\mathsf{SL}(*, \exists{:}\rightsquigarrow)$ is too long to be included in the present document. A technical appendix contains syntactic derivations omitted from the body of the paper.

2. Preliminaries

2.1. **Quantifier-free separation logic.** We present the quantifier-free separation logic $\mathsf{SL}(*, -\!\!*)$, that includes standard features such as the separating conjunction $*$, the separating implication $-\!\!*$ and closure under Boolean connectives. Let $\mathsf{VAR} = \{\mathtt{x}, \mathtt{y}, \ldots\}$ be a countably infinite set of *program variables*. The formulae φ of $\mathsf{SL}(*, -\!\!*)$ and its atomic formulae π are built from the grammars below where $\mathtt{x}, \mathtt{y} \in \mathsf{VAR}$.

$$\pi ::= \mathtt{x} = \mathtt{y} \mid \mathtt{x} \hookrightarrow \mathtt{y} \mid \mathtt{emp} \qquad\qquad \varphi ::= \pi \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi * \varphi \mid \varphi -\!\!* \varphi.$$

The connectives $\Rightarrow$, $\Leftrightarrow$ and $\vee$ are defined as usually. In the heaplet semantics, the formulae of $\mathsf{SL}(*, -\!\!*)$ are interpreted on *memory states* that are pairs (s, h) where $s : \mathsf{VAR} \to \mathsf{LOC}$ is a variable valuation (the *store*) from the set of program variables to a countably infinite set of *locations* $\mathsf{LOC} = \{\ell_0, \ell_1, \ell_2, \ldots\}$, whereas $h : \mathsf{LOC} \to_{\mathsf{fin}} \mathsf{LOC}$ is a partial function with finite domain (the *heap*). We write $\mathrm{dom}(h)$ to denote its domain and $\mathrm{ran}(h)$ to denote its range. A *memory cell* of h is understood as a pair of locations (ℓ, ℓ') such that $\ell \in \mathrm{dom}(h)$ and $\ell' = h(\ell)$. As usual, the heaps h_1 and h_2 are said to be *disjoint*, written $h_1 \sharp h_2$, if $\mathrm{dom}(h_1) \cap \mathrm{dom}(h_2) = \varnothing$; when this holds, we write $h_1 + h_2$ to denote the heap corresponding to the disjoint union of the graphs of h_1 and h_2, hence $\mathrm{dom}(h_1 + h_2) = \mathrm{dom}(h_1) \uplus \mathrm{dom}(h_2)$.

When the domains of h_1 and h_2 are not disjoint, the composition $h_1 + h_2$ is not defined. Moreover, we write $h' \sqsubseteq h$ to denote that $\mathrm{dom}(h') \subseteq \mathrm{dom}(h)$ and for all locations $\ell \in \mathrm{dom}(h')$, we have $h'(\ell) = h(\ell)$. If $h' \sqsubseteq h$ then h' is said to be a *subheap* of h. The satisfaction relation $\models$ is defined as follows (we omit standard clauses for the Boolean connectives $\neg$ and $\wedge$):

$$
\begin{array}{lcl}
(s,h) \models \mathtt{x} = \mathtt{y} & \stackrel{\text{def}}{\Leftrightarrow} & s(\mathtt{x}) = s(\mathtt{y}), \\
(s,h) \models \mathtt{emp} & \stackrel{\text{def}}{\Leftrightarrow} & \mathrm{dom}(h) = \varnothing, \\
(s,h) \models \mathtt{x} \hookrightarrow \mathtt{y} & \stackrel{\text{def}}{\Leftrightarrow} & s(\mathtt{x}) \in \mathrm{dom}(h) \text{ and } h(s(\mathtt{x})) = s(\mathtt{y}), \\
(s,h) \models \varphi_1 * \varphi_2 & \stackrel{\text{def}}{\Leftrightarrow} & \text{there are } h_1, h_2 \text{ such that } h_1 \sharp h_2,\ (h_1 + h_2) = h, \\
 & & (s,h_1) \models \varphi_1 \text{ and } (s,h_2) \models \varphi_2, \\
(s,h) \models \varphi_1 \mathrel{-\!\!*} \varphi_2 & \stackrel{\text{def}}{\Leftrightarrow} & \text{for all } h_1 \text{ such that } h_1 \sharp h \text{ and } (s,h_1) \models \varphi_1, \\
 & & \text{we have } (s, h + h_1) \models \varphi_2.
\end{array}
$$

We denote with $\bot$ the contradiction $\mathtt{x} \neq \mathtt{x}$, and with $\top$ its negation $\neg\bot$. The septraction operator $\mathrel{-\!\!\circledast}$ (kind of dual of $\mathrel{-\!\!*}$), defined by $\varphi \mathrel{-\!\!\circledast} \psi \stackrel{\text{def}}{=} \neg(\varphi \mathrel{-\!\!*} \neg\psi)$, has the following semantics:

$$(s,h) \models \varphi \mathrel{-\!\!\circledast} \psi \stackrel{\text{def}}{\Leftrightarrow} \text{there is a heap } h' \text{ such that } h \sharp h',\ (s,h') \models \varphi, \text{ and } (s, h + h') \models \psi.$$

We adopt the standard precedence between classical connectives, and extend it for the connectives of separation logic as follows: $\{\neg\} > \{\wedge, \vee, *\} > \{\Rightarrow, \mathrel{-\!\!*}, \mathrel{-\!\!\circledast}\} > \{\Leftrightarrow\}$. Notice that the separating conjunction $*$ has a higher precedence than the separating implication $\mathrel{-\!\!*}$, and it has the same precedence as the (classical) conjunction $\wedge$. For instance, $\varphi * \psi \Rightarrow \chi$ and $\neg\varphi \mathrel{-\!\!*} \psi * \psi$ stand for $(\varphi * \psi) \Rightarrow \chi$ and $(\neg\varphi) \mathrel{-\!\!*} (\psi * \psi)$, respectively.

A formula φ is *valid* if $(s,h) \models \varphi$ for all memory states (s,h) (and we write $\models \varphi$). For a complete description of separation logic, see e.g. [Rey02]. Given a set of formulae Γ, we write $\Gamma \models \varphi$ (semantical entailment) whenever $(s,h) \models \varphi$ holds for every memory state (s,h) satisfying every formula in Γ.

It is worth noting that quantifier-free $\mathsf{SL}(*, \mathrel{-\!\!*})$ axiomatised in the paper admits a PSPACE-complete validity problem, see e.g. [COY01], and should not be confused with propositional separation logic with the stack-heap models shown undecidable in [BK14, Corollary 5.1] (see also [DD15, Section 4]), in which there are propositional variables interpreted by sets of memory states.

2.2. **Core formulae.** We introduce the following well-known shortcuts, that play an important role in the sequel. Let $\mathtt{x} \in \mathsf{VAR}$ and $\beta \in \mathbb{N}$.

Shortcut:	Definition:		Semantics:
$\mathtt{alloc}(\mathtt{x})$	$\stackrel{\text{def}}{=}\ (\mathtt{x} \hookrightarrow \mathtt{x}) \mathrel{-\!\!*} \bot$		$(s,h) \models \mathtt{alloc}(\mathtt{x})$ iff $s(\mathtt{x}) \in \mathrm{dom}(h)$
$\mathtt{size} \geqslant \beta$	$\stackrel{\text{def}}{=}\begin{cases} \top & \text{if } \beta = 0 \\ \neg\mathtt{emp} & \text{if } \beta = 1 \\ \neg\mathtt{emp} * \mathtt{size} \geqslant \beta{-}1 & \text{otherwise} \end{cases}$		$(s,h) \models \mathtt{size} \geqslant \beta$ iff $\mathrm{card}(\mathrm{dom}(h)) \geqslant \beta$

We use $\mathtt{size}{=}\beta$ as a shorthand for $\mathtt{size}{\geqslant}\beta \wedge \neg\mathtt{size}{\geqslant}\beta{+}1$. We also write $\mathrm{card}(X)$ to denote the cardinality of the set X.

The *core formulae* are expressions of the form $\mathtt{x} = \mathtt{y}$, $\mathtt{alloc}(\mathtt{x})$, $\mathtt{x} \hookrightarrow \mathtt{y}$ and $\mathtt{size} \geqslant \beta$, where $\mathtt{x}, \mathtt{y} \in \mathsf{VAR}$ and $\beta \in \mathbb{N}$. As we can see, the core formulae are simple $\mathsf{SL}(*, \mathrel{-\!\!*})$ formulae.

It is well-known, see e.g. [Yan01, Loz04a], that these formulae capture essential properties of the memory states. In particular, every formula of $\mathsf{SL}(*, -\!\!*)$ is logically equivalent to a Boolean combination of core formulae [Loz04a].

As a simple but crucial insight, since the core formulae are formulae of $\mathsf{SL}(*, -\!\!*)$, we can freely use them to help us defining the proof system for $\mathsf{SL}(*, -\!\!*)$, and preventing us from going outside the original language. Having this in mind, the resulting proof system is Hilbert-style and completely internal (the formal definition of these types of systems is recalled below).

Given $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$ and $\alpha \in \mathbb{N}$, we define $\mathsf{Core}(\mathtt{X}, \alpha)$ as the set

$$\{\mathtt{x} = \mathtt{y},\ \mathtt{alloc}(\mathtt{x}),\ \mathtt{x} \hookrightarrow \mathtt{y},\ \mathtt{size} \geqslant \beta \mid \mathtt{x}, \mathtt{y} \in \mathtt{X},\ \beta \in [0, \alpha]\}.$$

$\mathsf{Bool}(\mathsf{Core}(\mathtt{X}, \alpha))$ is defined as the set of Boolean combinations of formulae from $\mathsf{Core}(\mathtt{X}, \alpha)$, whereas $\mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \alpha))$ is the set of conjunctions of literals built upon $\mathsf{Core}(\mathtt{X}, \alpha)$. As usual, a *literal* is understood as a core formula or its negation. Let $\varphi = L_1 \wedge \cdots \wedge L_n \in \mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \alpha))$ be a conjunction of literals $L_1, \ldots, L_n$. We write $\mathsf{Lt}(\varphi)$ to denote $\{L_1, \ldots, L_n\}$. In forthcoming developments, we are interested in the maximum β (if any) of formulae of the form $\mathtt{size} \geqslant \beta$ occurring positively in a conjunction of literals, if any. For this reason, we write $\max_{\mathtt{size}}(\varphi)$ for $\max(\{\beta \in \mathbb{N} \mid \mathtt{size} \geqslant \beta \in \mathsf{Lt}(\varphi)\} \cup \{0\})$. For instance, given $\varphi = \mathtt{alloc}(\mathtt{x}) \wedge \mathtt{size} \geqslant 2 \wedge \neg\mathtt{size} \geqslant 4$, we have $\mathsf{Lt}(\varphi) = \{\mathtt{alloc}(\mathtt{x}), \mathtt{size} \geqslant 2, \neg\mathtt{size} \geqslant 4\}$, and $\max_{\mathtt{size}}(\varphi) = 2$. Given two conjunctions of literals $\varphi \in \mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \alpha_1))$ and $\psi \in \mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \alpha_2))$, $\psi \subseteq_{\mathsf{Lt}} \varphi$ stands for $\mathsf{Lt}(\psi) \subseteq \mathsf{Lt}(\varphi)$. Finally, we introduce a few more shortcuts and we write

- $\chi \subseteq_{\mathsf{Lt}} \{\varphi \mid \psi\}$ for "$\chi \subseteq_{\mathsf{Lt}} \varphi$ or $\chi \subseteq_{\mathsf{Lt}} \psi$",
- $\chi \subseteq_{\mathsf{Lt}} \{\varphi\,;\psi\}$ for "$\chi \subseteq_{\mathsf{Lt}} \varphi$ and $\chi \subseteq_{\mathsf{Lt}} \psi$",
- $\{\varphi \mid \psi\} \subseteq_{\mathsf{Lt}} \chi$ for "$\varphi \subseteq_{\mathsf{Lt}} \chi$ or $\psi \subseteq_{\mathsf{Lt}} \chi$".

Given a finite set of formulae $\Gamma = \{\varphi_1, \ldots, \varphi_n\}$, we write $\bigwedge \Gamma$ as a shorthand for $\varphi_1 \wedge \cdots \wedge \varphi_n$. Similarly, $*\Gamma$ stands for $\varphi_1 * \ldots * \varphi_n$. It is important to notice that, similarly to the classical conjunction, the separating conjunction $*$ is associative and commutative (see the axioms $\mathbf{(A_8^*)}$ and $\mathbf{(A_7^*)}$ in Figure 1), and therefore the semantics of $*\Gamma$ is uniquely defined, regardless of the choice of ordering for $\varphi_1, \ldots, \varphi_n$.

2.3. **Hilbert-style proof systems.** A *Hilbert-style proof system* $\mathcal{H}$ is defined as a set of tuples $((\Phi_1, \ldots, \Phi_n), \Psi)$ with $n \geqslant 0$, where $\Phi_1, \ldots, \Phi_n, \Psi$ are *formula schemata* (a.k.a *axiom schemata*). When $n \geqslant 1$, $((\Phi_1, \ldots, \Phi_n), \Psi)$ is called an *inference rule*, otherwise it is an *axiom*. As usual, formula schemata generalise the notion of formulae by allowing metavariables for formulae (typically φ, ψ, χ), for program variables (typically $\mathtt{x}, \mathtt{y}, \mathtt{z}$) or for any type of syntactic objects in formulae, depending on the context. The set of formulae *derivable* from $\mathcal{H}$ is the least set S such that for all $((\Phi_1, \ldots, \Phi_n), \Psi) \in \mathcal{H}$ and for all substitutions σ, if $\Phi_1\sigma, \ldots, \Phi_n\sigma \in S$ then $\Psi\sigma \in S$. We write $\vdash_{\mathcal{H}} \varphi$ if φ is derivable from $\mathcal{H}$. A proof system $\mathcal{H}$ is *sound* if all derivable formulae are valid. $\mathcal{H}$ is *complete* if all valid formulae are derivable. We say that $\mathcal{H}$ is *adequate* whenever it is both sound and complete. Lastly, $\mathcal{H}$ is *strongly complete* whenever for all sets of formulae Γ and formulae φ, we have $\Gamma \models \varphi$ (semantical entailment) if and only if $\vdash_{\mathcal{H} \cup \Gamma} \varphi$.

Interestingly enough, there is no strongly complete proof system for $\mathsf{SL}(*, -\!\!*)$, as strong completeness implies compactness and separation logic is not compact. Indeed, $\{\mathtt{size} \geqslant \beta \mid \beta \in \mathbb{N}\}$ is unsatisfiable, as heaps have finite domains, but all finite subsets

$(\mathbf{A_1^C})$ $\mathtt{x} = \mathtt{x}$

$(\mathbf{A_2^C})$ $\varphi \wedge \mathtt{x} = \mathtt{y} \Rightarrow \varphi[\mathtt{y} \leftarrow \mathtt{x}]$

$(\mathbf{A_3^C})$ $\mathtt{x} \hookrightarrow \mathtt{y} \Rightarrow \mathtt{alloc(x)}$

$(\mathbf{A_4^C})$ $\mathtt{x} \hookrightarrow \mathtt{y} \wedge \mathtt{x} \hookrightarrow \mathtt{z} \Rightarrow \mathtt{y} = \mathtt{z}$

$(\mathbf{A_7^*})$ $(\varphi * \psi) \Leftrightarrow (\psi * \varphi)$

$(\mathbf{A_8^*})$ $(\varphi * \psi) * \chi \Leftrightarrow \varphi * (\psi * \chi)$

$(\mathbf{A_{11}^*})$ $\varphi \Leftrightarrow \varphi * \mathtt{emp}$

$(\mathbf{A_{13}^*})$ $\mathtt{alloc(x)} * \mathtt{alloc(x)} \Leftrightarrow \bot$

$(\mathbf{A_{14}^*})$ $\mathtt{e} * \top \Rightarrow \mathtt{e} \blacktriangleleft [\mathtt{e} \in \{\neg\mathtt{emp}, \mathtt{x} = \mathtt{y}, \mathtt{x} \neq \mathtt{y}, \mathtt{x} \hookrightarrow \mathtt{y}\}]$

$(\mathbf{A_{15}^*})$ $\neg\mathtt{alloc(x)} * \neg\mathtt{alloc(x)} \Rightarrow \neg\mathtt{alloc(x)}$

$(\mathbf{A_{16}^*})$ $(\mathtt{alloc(x)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y}) * \top \Rightarrow \neg \mathtt{x} \hookrightarrow \mathtt{y}$

$(\mathbf{A_{17}^*})$ $\mathtt{alloc(x)} \Rightarrow (\mathtt{alloc(x)} \wedge \mathtt{size} = 1) * \top$

$(\mathbf{A_{18}^*})$ $\neg\mathtt{emp} \Rightarrow \mathtt{size} = 1 * \top$

$(\mathbf{A_{19}^*})$ $\neg\mathtt{size} \geqslant \beta_1 * \neg\mathtt{size} \geqslant \beta_2 \Rightarrow \neg\mathtt{size} \geqslant \beta_1 + \beta_2 \dot{-} 1$

$(\mathbf{A_{20}^*})$ $\mathtt{alloc(x)} \wedge \mathtt{alloc(y)} \wedge \mathtt{x} \neq \mathtt{y} \Rightarrow \mathtt{size} \geqslant 2$

$(\mathbf{A_{21}^{-*}})$ $(\mathtt{size} = 1 \wedge \bigwedge_{\mathtt{x} \in \mathtt{X}} \neg\mathtt{alloc(x)}) \mathbin{-\!\circledast} \top \blacktriangleleft [\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}]$

$(\mathbf{A_{22}^{-*}})$ $\neg\mathtt{alloc(x)} \Rightarrow (\mathtt{x} \hookrightarrow \mathtt{y} \wedge \mathtt{size} = 1 \mathbin{-\!\circledast} \top)$

$(\mathbf{A_{23}^{-*}})$ $\neg\mathtt{alloc(x)} \Rightarrow ((\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \wedge \bigwedge_{\mathtt{y} \in \mathtt{X}} \neg \mathtt{x} \hookrightarrow \mathtt{y}) \mathbin{-\!\circledast} \top) \blacktriangleleft [\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}]$

$*$**-Intro**: $\dfrac{\varphi \Rightarrow \chi}{\varphi * \psi \Rightarrow \chi * \psi}$ $\qquad$ $*$**-Adj**: $\dfrac{\varphi * \psi \Rightarrow \chi}{\varphi \Rightarrow (\psi \mathbin{-\!*} \chi)}$ $\qquad$ $-\!*$**-Adj**: $\dfrac{\varphi \Rightarrow (\psi \mathbin{-\!*} \chi)}{\varphi * \psi \Rightarrow \chi}$

(axioms and modus ponens from propositional calculus are omitted)

Figure 1: The proof system $\mathcal{H}_{\mathsf{C}}(*, -\!*)$.

of it are satisfiable. Even for the weaker notion of completeness, deriving an Hilbert-style axiomatisation for $\mathsf{SL}(*, -\!*)$ remains challenging. Indeed, the satisfiability problem for $\mathsf{SL}(*, -\!*)$ reduces to its validity problem, making $\mathsf{SL}(*, -\!*)$ an unusual logic from a proof-theoretical point of view. Let us develop a bit further this point.

Let φ be a formula built over program variables in $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$, and let $\approx$ be an equivalence relation on $\mathtt{X}$. The formula $\psi_{\approx} \stackrel{\text{def}}{=} (\mathtt{emp} \wedge \bigwedge_{\mathtt{x} \approx \mathtt{y}} \mathtt{x} = \mathtt{y} \wedge \bigwedge_{\mathtt{x} \not\approx \mathtt{y}} \mathtt{x} \neq \mathtt{y}) \Rightarrow (\varphi \mathbin{-\!\circledast} \top)$ can be shown to be valid iff for every store s agreeing on $\approx$, there is a heap h such that $(s, h) \models \varphi$. It is known that for all stores s, s' agreeing on $\approx$, and every heap h, the memory states (s, h) and (s', h) satisfy the same set of formulae having variables from $\mathtt{X}$. Since the antecedent of $\psi_{\approx}$ is satisfiable, we conclude that $\psi_{\approx}$ is valid iff there are a store s agreeing on $\approx$ and a heap h such that $(s, h) \models \varphi$. To check whether φ is satisfiable, it is sufficient to find an equivalence relation $\approx$ on $\mathtt{X}$ such that $\psi_{\approx}$ is valid. As the number of equivalence relations on $\mathtt{X}$ is finite, we obtain a Turing reduction from satisfiability to validity. Consequently, it is not possible to define sound and complete axiom systems for any extension of $\mathsf{SL}(*, -\!*)$ admitting an undecidable validity problem (as long as there is a reduction from satisfiability to validity, as above). A good example is the logic $\mathsf{SL}(*, -\!*, \mathtt{ls})$ [DLM18b] (extension of $\mathsf{SL}(*, -\!*)$ with the well-known list-segment predicate $\mathtt{ls}$); see also the first-order separation logic in [BDL12]. Indeed, to obtain a sound and complete axiom system, the validity problem has to be recursively enumerable (r.e.). However, this would imply that the satisfiability problem is also r.e.. As a formula φ is not valid if and only if $\neg\varphi$ is satisfiable, we then conclude that the set of valid formulae is recursive, hence decidable, a contradiction.

3. Hilbert-style proof system for $\mathsf{SL}(*, -\!*)$

In Figure 1, we present the proof system $\mathcal{H}_{\mathsf{C}}(*, -\!*)$ that shall be shown to be sound and complete for quantifier-free separation logic $\mathsf{SL}(*, -\!*)$. $\mathcal{H}_{\mathsf{C}}(*, -\!*)$ and all the subsequent

fragments of $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ contain the axiom schemata and modus ponens for the propositional calculus (we omit these rules in the presentation). In the axioms $(\mathbf{A}^{*}_{\mathbf{14}})$, $(\mathbf{A}^{-\!\!*}_{\mathbf{21}})$ and $(\mathbf{A}^{-\!\!*}_{\mathbf{23}})$, the notation $\varphi \blacktriangleleft [\mathcal{B}]$ refers to the axiom schema φ assuming that the Boolean condition $\mathcal{B}$ holds. We highlight the fact that, in these three axioms, $\mathcal{B}$ is a simple syntactical condition. In the axiom $(\mathbf{A}^{*}_{\mathbf{19}})$, $a \dot{-} b$, where $a, b \in \mathbb{N}$, stands for $\max(0, a - b)$.

Though the full proof system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ is presented quite early in the paper, its final design remains the outcome of a refined analysis on principles behind $\mathsf{SL}(*, -\!\!*)$ tautologies. Fortunately, we do not start from scratch as the calculus must contain the axioms and rules from the Hilbert-style proof system for Boolean BI [GLW06]. At first glance the system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ may seem quite arbitrary, but the role of the different axioms shall become clearer during the paper. In designing the system, we tried to define axioms that are as simple as possible, which helps highlighting the most fundamental properties of $\mathsf{SL}(*, -\!\!*)$. Note that we have not formally proved that our proof system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ is minimal (though we have tried our best to have a small amount of small axioms). Such an investigation would be out of the scope of the paper, mainly for lack of space. The standard way to proceed would be to design models different from memory states and to establish that all axioms but one are valid (which would prove that this axiom is needed when all the other axioms are present).

We insist: the core formulae in $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ should be understood as mere abbreviations, which makes all the axioms in Figure 1 belong to the original language of $\mathsf{SL}(*, -\!\!*)$. In order to show the completeness of $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$, we first establish the completeness for subsystems of $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$, with respect to syntactical fragments of $\mathsf{SL}(*, -\!\!*)$. In particular, we consider

- $\mathcal{H}_{\mathsf{C}}$: an adequate proof system for the propositional logic of core formulae (see Figure 4),
- $\mathcal{H}_{\mathsf{C}}(*)$: an extension of $\mathcal{H}_{\mathsf{C}}$ that is adequate for the logic $\mathsf{SL}(*, \mathtt{alloc})$, i.e. the logic obtained from $\mathsf{SL}(*, -\!\!*)$ by removing the separating implication $-\!\!*$ at the price of adding the formula $\mathtt{alloc(x)}$ (see Figure 5).
- The full $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$, which can be seen as an extension of $\mathcal{H}_{\mathsf{C}}(*)$ that allows to reason about the separating implication (see Figure 7).

For the completeness of $\mathcal{H}_{\mathsf{C}}$ and $\mathcal{H}_{\mathsf{C}}(*)$, we add intermediate axioms that reveal to be useless when the full proof system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ is considered, as they become derivable. By convention, the axioms whose name is of the form $A^{?}_{i}$ are axioms that remain in $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ (see Figure 1) whereas those named $I^{?}_{i}$ are intermediate axioms that are instrumental for the proof of completeness of a subsystem among $\mathcal{H}_{\mathsf{C}}$ and $\mathcal{H}_{\mathsf{C}}(*)$ (and therefore none of them occur in Figure 1). The numbering of the axioms in Figure 1 is not consecutive, as intermediate axioms shall be placed within the holes. It is worth noting that the axiom $(\mathbf{A}^{*}_{\mathbf{13}})$ had an intermediate status in [DLM20] but we realised that actually this axiom does need to be considered as a first-class axiom in the proof system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$.

The choice of introducing $\mathcal{H}_{\mathsf{C}}$ and $\mathcal{H}_{\mathsf{C}}(*)$ naturally follows from the main steps required for the completeness of $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$. In particular, the main "task" of $\mathcal{H}_{\mathsf{C}}(*)$ is to produce a bottom-up elimination of the separating conjunction $*$, at the price of introducing Boolean combinations of core formulae, which can be proved valid thanks to $\mathcal{H}_{\mathsf{C}}$. Similarly, the axioms and rules added to $\mathcal{H}_{\mathsf{C}}(*)$ to define $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ are dedicated to perform a bottom-up elimination of the separating implication. A merit of this methodology is that only the completeness of the calculus $\mathcal{H}_{\mathsf{C}}$ is proved using the standard countermodel method. The additional steps required to prove the completeness of $\mathcal{H}_{\mathsf{C}}(*)$ and $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ are (almost) completely syntactical. For instance, to show the completeness of $\mathcal{H}_{\mathsf{C}}(*)$, we consider arbitrary Boolean combinations of core formulae φ and ψ, and exhibiting a Boolean combination of

core formulae χ such that $\varphi * \psi \Leftrightarrow \chi$ is valid. We show that this validity can be *syntactically* proved within $\mathcal{H}_{\mathsf{C}}(*)$, and then rely on the fact that $\mathcal{H}_{\mathsf{C}}$ is complete for Boolean combination of core formulae to deduce that $\mathcal{H}_{\mathsf{C}}(*)$ is complete for $\mathsf{SL}(*, \mathtt{alloc})$.

Along the paper, we shall have the opportunity to explain the intuition between the axioms and rules. Below, we provide a few hints. The axioms $\mathbf{(A_1^{\mathsf{C}})}$– $\mathbf{(A_4^{\mathsf{C}})}$ deal with the core formulae and are quite immediate to grasp. More interestingly, whereas the axioms $\mathbf{(A_7^*)}$–$\mathbf{(A_{11}^*)}$ are quite general about separating conjunction and are inherited from Boolean BI, the axioms $\mathbf{(A_{14}^*)}$–$\mathbf{(A_{20}^*)}$ state how separating conjunction behaves with the core formulae. As for Boolean combinations of core formulae involved in the axioms $\mathbf{(A_1^{\mathsf{C}})}$– $\mathbf{(A_4^{\mathsf{C}})}$, these axioms $\mathbf{(A_{14}^*)}$–$\mathbf{(A_{20}^*)}$ are also not difficult to understand. Besides, the inference rules $*$**-Adj** and $-\!\!*$**-Adj** simply reflect that separating conjunction and separating implication are adjoint operators, and are taken from Boolean BI, see e.g. [GLW06]. The axioms $\mathbf{(A_{21}^{-\!*})}$–$\mathbf{(A_{23}^{-\!*})}$ dedicated to the interaction between the separating implication and core formulae are expressed with the help of the septraction operator $-\!\circledast$ to ease the understanding but as well-known, septraction is defined with the help of the separating implication and Boolean negation. For instance, the axiom $\mathbf{(A_{22}^{-\!*})}$ states that it is always possible to add some one-memory-cell heap h' to some heap h while none of the variables from a finite set $\mathtt{X}$ is allocated in h'. This natural property in our framework would not hold in general if LOC were not infinite. Obviously, the septraction $-\!\circledast$ is also understood as an abbreviation.

As a sanity check, we show that the proof system $\mathcal{H}_{\mathsf{C}}(*, -\!*)$ is sound with respect to $\mathsf{SL}(*, -\!*)$. The proof does not pose any specific difficulty (as usual with most soundness proofs) but this is the opportunity for the reader to further get familiar with the axioms and rules from $\mathcal{H}_{\mathsf{C}}(*, -\!*)$.

Lemma 3.1. *$\mathcal{H}_{\mathsf{C}}(*, -\!*)$ is sound.*

The validity of the axioms $\mathbf{(A_1^{\mathsf{C}})}$, $\mathbf{(A_2^{\mathsf{C}})}$, $\mathbf{(A_3^{\mathsf{C}})}$ and $\mathbf{(A_4^{\mathsf{C}})}$ is straightforward. Moreover, the validity of the axioms $\mathbf{(A_7^*)}$, $\mathbf{(A_8^*)}$ and $\mathbf{(A_{11}^*)}$ and the three inference rules ($*$**-Intro**, $*$**-Adj** and $-\!*$**-Adj**) is inherited from Boolean BI (see [BV14] and [GLW06, Section 2]). Below, we show the validity of the remaining axioms, thus proving Lemma 3.1.

Validity of the axiom $\mathbf{(A_{13}^*)}$. Let us show that $(\mathtt{alloc(x)} * \mathtt{alloc(x)})$ is not satisfiable. *Ad absurdum*, suppose there is a memory state (s, h) such that $(s, h) \models (\mathtt{alloc(x)} * \mathtt{alloc(x)})$. By definition of $\models$, there are h_1, h_2 such that $h_1 \bot h_2$, $(h_1 + h_2) = h$, $(s, h_1) \models \mathtt{alloc(x)}$ and $(s, h_2) \models \mathtt{alloc(x)}$. Thus, $s(\mathtt{x}) \in \mathrm{dom}(h_1)$ and $s(\mathtt{x}) \in \mathrm{dom}(h_2)$, which leads to a contradiction with $h_1 \bot h_2$. □

Validity of the axiom $\mathbf{(A_{14}^*)}$. The proof of the validity of every instantiation of $\mathbf{(A_{14}^*)}$ is similar (and quite easy), therefore we show just the case with $\mathtt{x} \hookrightarrow \mathtt{y} * \top \Rightarrow \mathtt{x} \hookrightarrow \mathtt{y}$. Suppose $(s, h) \models \mathtt{x} \hookrightarrow \mathtt{y} * \top$. Then, there is a subheap $h_1 \sqsubseteq h$ such that $(s, h_1) \models \mathtt{x} \hookrightarrow \mathtt{y}$. Hence, $h_1(s(\mathtt{x})) = s(\mathtt{y})$. As $h_1 \sqsubseteq h$, we obtain $h(s(\mathtt{x})) = s(\mathtt{y})$, which implies $(s, h) \models \mathtt{x} \hookrightarrow \mathtt{y}$. □

Validity of the axiom $\mathbf{(A_{15}^*)}$. Suppose $(s, h) \models \neg\mathtt{alloc(x)} * \neg\mathtt{alloc(x)}$. Then, there are two disjoint heaps h_1, h_2 such that $h = h_1 + h_2$, $(s, h_1) \models \neg\mathtt{alloc(x)}$ and $(s, h_2) \models \neg\mathtt{alloc(x)}$. Then $s(\mathtt{x}) \notin \mathrm{dom}(h_1)$ and $s(\mathtt{x}) \notin \mathrm{dom}(h_2)$. Since $h = h_1 + h_2$, $\mathrm{dom}(h) = \mathrm{dom}(h_1) \cup \mathrm{dom}(h_2)$ and therefore $s(\mathtt{x}) \notin \mathrm{dom}(h)$. We conclude that $(s, h) \models \neg\mathtt{alloc(x)}$. □

Validity of the axiom $\mathbf{(A_{16}^*)}$. Suppose $(s, h) \models (\mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}) * \top$. Then there is a subheap $h_1 \sqsubseteq h$ such that $(s, h_1) \models \mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}$. Hence, $s(\mathtt{x}) \in \mathrm{dom}(h_1)$ and

1	$\mathtt{emp} \Rightarrow \neg\mathtt{size} \geqslant 1$	**($\neg\neg$I)** and def. of $\mathtt{size} \geqslant 1$
2	$\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \Rightarrow \neg\mathtt{size} \geqslant 2$	**($\wedge$Er)**
3	$\mathtt{emp} * (\mathtt{alloc(x)} \wedge \mathtt{size} = 1) \Rightarrow \neg\mathtt{size} \geqslant 1 * \neg\mathtt{size} \geqslant 2$	$*$**-Ilr**, 1, 2
4	$\neg\mathtt{size} \geqslant 1 * \neg\mathtt{size} \geqslant 2 \Rightarrow \neg\mathtt{size} \geqslant 2$	**($\mathbf{A^*_{19}}$)**
5	$\mathtt{emp} * (\mathtt{alloc(x)} \wedge \mathtt{size} = 1) \Rightarrow \neg\mathtt{size} \geqslant 2$	$\Rightarrow$**-Tr**, 3, 4
6	$\mathtt{emp} \Rightarrow \big(\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2\big)$	$*$**-Adj**, 5

Figure 2: A proof of $\mathtt{emp} \Rightarrow \big((\mathtt{alloc(x)} \wedge \mathtt{size} = 1) \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2\big)$.

$h_1(s(\mathtt{x})) \neq s(\mathtt{y})$. As $h_1 \sqsubseteq h$, we obtain $s(\mathtt{x}) \in \mathrm{dom}(h)$ and $h(s(\mathtt{x})) \neq s(\mathtt{y})$ which by definition implies $(s,h) \models \neg\mathtt{x} \hookrightarrow \mathtt{y}$. □

Validity of the axiom **($\mathbf{A^*_{17}}$)**. Suppose $(s,h) \models \mathtt{alloc(x)}$. Let $h_1 \stackrel{\text{def}}{=} \{s(\mathtt{x}) \mapsto h(s(\mathtt{x}))\}$ As $s(\mathtt{x}) \in \mathrm{dom}(h)$, $h_1 \sqsubseteq h$ and $(s,h_1) \models \mathtt{alloc(x)} \wedge \mathtt{size} = 1$. We define h_2 as the unique heap such that $h_2 + h_1 = h$. As $(s,h_2) \models \top$, we have $(s,h) \models (\mathtt{alloc(x)} \wedge \mathtt{size} = 1) * \top$. □

The proof of axiom **($\mathbf{A^*_{18}}$)** is similar to the one of **($\mathbf{A^*_{17}}$)**, and hence omitted herein.

Validity of the axiom **($\mathbf{A^*_{19}}$)**. Suppose $(s,h) \models \neg\mathtt{size} \geqslant \beta_1 * \neg\mathtt{size} \geqslant \beta_2$, where $\beta_1, \beta_2 \geqslant 0$. Since $\neg\mathtt{size} \geqslant 0$ is not satisfiable, this implies that necessarily $\beta_1, \beta_2 \geqslant 1$. Hence, the axiom **($\mathbf{A^*_{19}}$)** is trivially valid when $\beta_1 = 0$ or $\beta_2 = 0$. In the sequel, $\beta_1, \beta_2 \geqslant 1$. Then, there are heaps h_1, h_2 such that $h_1 \sharp h_2$, $h_1 + h_2 = h$, $(s,h_1) \models \neg\mathtt{size} \geqslant \beta_1$ and $(s,h_2) \models \neg\mathtt{size} \geqslant \beta_2$. By definition, $\mathrm{card}(\mathrm{dom}(h_1)) \leqslant \beta_1 - 1$ and $\mathrm{card}(\mathrm{dom}(h_2)) \leqslant \beta_2 - 1$. Since $\mathrm{dom}(h) = \mathrm{dom}(h_1) \cup \mathrm{dom}(h_2)$, we obtain $\mathrm{card}(\mathrm{dom}(h)) \leqslant \beta_1 + \beta_2 - 2$, which implies $(s,h) \models \neg\mathtt{size} \geqslant \beta_1 + \beta_2 \dot{-} 1$. □

Validity of the axiom **($\mathbf{A^*_{20}}$)**. Suppose $(s,h) \models \mathtt{alloc(x)} \wedge \mathtt{alloc(y)} \wedge \mathtt{x} \neq \mathtt{y}$. By definition, $s(\mathtt{x}) \neq s(\mathtt{y})$, and $s(\mathtt{x}), s(\mathtt{y}) \in \mathrm{dom}(h)$. Hence, $\mathrm{card}(\mathrm{dom}(h)) \geqslant 2$, and $(s,h) \models \mathtt{size} \geqslant 2$. □

Validity of the axiom **($\mathbf{A^{-\!*}_{21}}$)**. Let $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$ and (s,h) be a memory state. Let h_1 be a heap of size one such that $h_1(\ell) = \ell$ for some $\ell \notin \mathrm{dom}(h) \cup s(\mathtt{X})$. We write $s(\mathtt{X})$ to denote the set $\{s(\mathtt{x}) \mid \mathtt{x} \in \mathtt{X}\}$. Trivially $(s,h_1) \models \mathtt{size} = 1 \wedge \bigwedge_{\mathtt{x}\in\mathtt{X}} \neg\mathtt{alloc(x)}$. Moreover $h_1 \sharp h$ holds, hence $h_1 + h_2$ is defined and $(s, h + h_1) \models \top$. Then, $(s,h) \models (\mathtt{size} = 1 \wedge \bigwedge_{\mathtt{x}\in\mathtt{X}} \neg\mathtt{alloc(x)}) \mathrel{-\!\!\circledast} \top$. □

Validity of the axiom **($\mathbf{A^{-\!*}_{22}}$)**. Suppose $(s,h) \models \neg\mathtt{alloc(x)}$. Let h_1 be the heap of size one such that $h_1(s(\mathtt{x})) = s(\mathtt{y})$. Trivially, $(s,h_1) \models \mathtt{x} \hookrightarrow \mathtt{y} \wedge \mathtt{size} = 1$. Moreover, as $s(\mathtt{x}) \notin \mathrm{dom}(h)$, $h_1 \sharp h$ holds. Therefore, $h_1 + h$ is defined, and $(s, h + h_1) \models \top$. Then, $(s,h) \models (\mathtt{x} \hookrightarrow \mathtt{y} \wedge \mathtt{size} = 1) \mathrel{-\!\!\circledast} \top$. □

Validity of the axiom **($\mathbf{A^{-\!*}_{23}}$)**. Suppose $(s,h) \models \neg\mathtt{alloc(x)}$. Let $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$ and $h_1 \stackrel{\text{def}}{=} \{s(\mathtt{x}) \mapsto \ell\}$, where $\ell \notin s(\mathtt{X})$. Hence, $(s,h_1) \models \mathtt{alloc(x)} \wedge \mathtt{size} = 1 \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}} \neg\mathtt{x} \hookrightarrow \mathtt{y}$. Since $s(\mathtt{x}) \notin \mathrm{dom}(h)$, $h_1 \sharp h$. Therefore, the heap $h + h_1$ is defined and $(s, h + h_1) \models \top$. Then, $(s,h) \models (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}} \neg\mathtt{x} \hookrightarrow \mathtt{y}) \mathrel{-\!\!\circledast} \top$. □

Example 3.2. To further familiarise with the axioms and the rules of $\mathcal{H}_{\mathsf{C}}(*, \mathrel{-\!\!*})$, in Figure 2, we present a proof of $\mathtt{emp} \Rightarrow \big(\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2\big)$. In the proof, a line "$j \mid \chi \;\; A, i_1, \ldots, i_k$" states that χ is a theorem denoted by the index j and derivable by the

axiom or the rule A. If A is a rule, the indices $i_1, \ldots, i_k < j$ denote the theorems used as premises in order to derive χ. When a formula is obtained as a propositional tautology or by propositional reasoning from other formulae, we may write "PC" (standing for short 'Propositional Calculus'). Similarly, we provide any useful piece of information justifying the derivation, such as "Ind. hypothesis", "See ..." or "Previously derived". In the example, we use the rule $*$**-Adj**, which together with the rule $-\!\!*$**-Adj** states that the connectives $*$ and $-\!\!*$ are adjoint operators, as well as the axiom $\mathbf{(A^*_{19})}$, stating that $\mathrm{card}(\mathrm{dom}(h)) \leqslant \beta_1+\beta_2$ holds whenever a heap h can be split into two subheaps whose domains have less than β_1+1 and β_2+1 elements, respectively. We also use the following theorems and rules:

$\mathbf{(\wedge Er)}\ \psi \wedge \varphi \Rightarrow \varphi$ $\qquad$ $\mathbf{(\neg\neg I)}\ \varphi \Rightarrow \neg\neg\varphi$ $\qquad$ $\Rightarrow$**-Tr**: $\dfrac{\varphi \Rightarrow \chi \quad \chi \Rightarrow \psi}{\varphi \Rightarrow \psi}$ $\qquad$ $*$**-Ilr**: $\dfrac{\varphi \Rightarrow \varphi' \quad \psi \Rightarrow \psi'}{\varphi * \psi \Rightarrow \varphi' * \psi'}$

The first two theorems and the first rule are derivable by pure propositional reasoning. By way of example, we show that the inference rule $*$**-Ilr** is admissible.

1	$\varphi \Rightarrow \varphi'$	Hypothesis	5	$\varphi' * \psi \Rightarrow \psi * \varphi'$	$\mathbf{(A^*_7)}$
2	$\psi \Rightarrow \psi'$	Hypothesis	6	$\psi' * \varphi' \Rightarrow \varphi' * \psi'$	$\mathbf{(A^*_7)}$
3	$\varphi * \psi \Rightarrow \varphi' * \psi$	$*$**-Intro**, 1	7	$\varphi * \psi \Rightarrow \psi * \varphi'$	$\Rightarrow$**-Tr**, 3, 5
4	$\psi * \varphi' \Rightarrow \psi' * \varphi'$	$*$**-Intro**, 2	8	$\varphi * \psi \Rightarrow \varphi' * \psi'$	$\Rightarrow$**-Tr** twice, 7, 4, 6

Remark 3.3. Note that an alternative proof of theorem 5 in Figure 2 consists in applying $\Rightarrow$**-Tr** to theorem 2 and $\mathtt{emp} * \big(\mathtt{alloc(x)} \wedge \mathtt{size}{=}1\big) \Rightarrow \mathtt{alloc(x)} \wedge \mathtt{size}{=}1$, which holds by the axioms $\mathbf{(A^*_{11})}$ and $\mathbf{(A^*_7)}$.

Example 3.4. In Figure 3, we develop the proof of $\mathtt{emp} \Rightarrow (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 -\!\!* \mathtt{size} = 1)$ as a more complete example. We use the following theorems and rules:

$\mathbf{(-\!\!*\wedge\text{-}DistrL)}\ (\varphi -\!\!* \psi) \wedge (\varphi -\!\!* \chi) \Rightarrow (\varphi -\!\!* \psi \wedge \chi)$ $\qquad$ $\mathbf{(\wedge \top IL)}\ \varphi \Rightarrow \top \wedge \varphi$ $\qquad$ $\wedge$**InfL**: $\dfrac{\varphi \Rightarrow \chi}{\varphi \wedge \psi \Rightarrow \chi \wedge \psi}$

The rightmost axiom and the only rule are derivable by propositional reasoning. We show the admissibility of the axiom $\mathbf{(-\!\!*\wedge\text{-}DistrL)}$.

1	$(\varphi \mathrel{-\!\!\circledast} \neg\psi \vee \neg\chi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \neg\psi) \vee (\varphi \mathrel{-\!\!\circledast} \neg\chi)$	$\mathbf{(I^{-\!\!*}_{6.3.8})}$, Lemma 6.3
2	$\neg(\varphi -\!\!* \neg(\neg\psi \vee \neg\chi)) \Rightarrow \neg(\varphi -\!\!* \neg\neg\psi) \vee \neg(\varphi -\!\!* \neg\neg\chi)$	Def. $-\!\!\circledast$, 1
3	$\neg(\varphi -\!\!* \psi \wedge \chi) \Rightarrow \neg(\varphi -\!\!* \psi) \vee \neg(\varphi -\!\!* \chi)$	Replacement of equivalents, 2
4	$(\varphi -\!\!* \psi) \wedge (\varphi -\!\!* \chi) \Rightarrow (\varphi -\!\!* \psi \wedge \chi)$	PC, 3

Main ingredients of the method. Before showing completeness of $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$, let us recall the key ingredients of the method we follow, not only to provide a vade mecum for axiomatising other separation logics (which, in the second part of [DLM20], we illustrate on the newly introduced logic $\mathsf{SL}(*, \exists{:}{\rightsquigarrow})$), but also to identify the essential features and where variations are still possible. The Hilbert-style axiomatisation of $\mathsf{SL}(*, -\!\!*)$ shall culminate with Theorem 6.5 that states the adequateness of the proof system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$.

In order to axiomatise $\mathsf{SL}(*, -\!\!*)$ internally, as already emphasised several times, the core formulae play an essential role. The main properties of these formulae is that their Boolean combinations capture the full logic $\mathsf{SL}(*, -\!\!*)$ [Loz04a] and all the core formulae can be expressed in $\mathsf{SL}(*, -\!\!*)$. Generally speaking, our axiom system naturally leads to a form

1	$\top * (\mathtt{alloc(x)} \wedge \mathtt{size} = 1) \Rightarrow (\mathtt{alloc(x)} \wedge \mathtt{size} = 1) * \top$	$\mathbf{(A_7^*)}$
2	$\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \Rightarrow \mathtt{size} \geqslant 1$	$\mathbf{(\wedge Er)}$
3	$(\mathtt{alloc(x)} \wedge \mathtt{size} = 1) * \top \Rightarrow \mathtt{size} \geqslant 1 * \top$	$*$**-Intro**, 2
4	$\mathtt{size} \geqslant 1 * \top \Rightarrow \mathtt{size} \geqslant 1$	$\mathbf{(A_{14}^*)}$ ($\mathtt{size} \geqslant 1 \stackrel{\text{def}}{=} \neg\mathtt{emp}$)
5	$\top * (\mathtt{alloc(x)} \wedge \mathtt{size} = 1) \Rightarrow \mathtt{size} \geqslant 1$	$\Rightarrow$**-Tr** twice, 1, 3, 4
6	$\top \Rightarrow (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \mathtt{size} \geqslant 1)$	$*$**-Adj**, 5
7	$\mathtt{emp} \Rightarrow (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2)$	See Example 3.2
8	$(\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2) \Rightarrow$ $\quad \top \wedge (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2)$	$\mathbf{(\wedge \top IL)}$
9	$\top \wedge (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2) \Rightarrow$ $\quad \big((\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \mathtt{size} \geqslant 1) \wedge$ $\quad (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2)\big)$	$\wedge$**-InfL**, 6
10	$\big((\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \mathtt{size} \geqslant 1) \wedge$ $\quad (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2)\big) \Rightarrow$ $\quad (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \mathtt{size} = 1)$	$\mathbf{(-\!\!*\wedge\text{-}DistrL)}$ + Def. size
11	$(\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \neg\mathtt{size} \geqslant 2) \Rightarrow$ $\quad (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \mathtt{size} = 1)$	$\Rightarrow$**-Tr** twice, 8, 9, 10
12	$\mathtt{emp} \Rightarrow (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \mathtt{size} = 1)$	$\Rightarrow$**-Tr**, 7, 11

(recall that $\mathtt{size} = \beta$ is a shortcut for $\mathtt{size} \geqslant \beta \wedge \neg\mathtt{size} \geqslant \beta{+}1$)

Figure 3: A proof of $\mathtt{emp} \Rightarrow (\mathtt{alloc(x)} \wedge \mathtt{size} = 1 \mathrel{-\!\!*} \mathtt{size} = 1)$.

of constructive completeness, as advocated in [Dou17, Lüc18]: the axiomatisation provides proof-theoretical means to transform any formula into an equivalent Boolean combination of core formulae, and it contains also a part dedicated to the derivation of valid Boolean combinations of core formulae (understood as a syntactical fragment of $\mathsf{SL}(*, \mathrel{-\!\!*})$). What is specific to each logic is the design of the set of core formulae and in the case of $\mathsf{SL}(*, \mathrel{-\!\!*})$, this was already known since [Loz04a].

Derivations in the proof system $\mathcal{H}_{\mathsf{C}}(*, \mathrel{-\!\!*})$ shall simulate the bottom-up elimination of separating connectives (see forthcoming Lemmata 5.5 and 6.2) when the arguments are two Boolean combinations of core formulae. To do so, $\mathcal{H}_{\mathsf{C}}(*, \mathrel{-\!\!*})$ contains axiom schemas that perform such an elimination in multiple "small-step" derivations, e.g. by deriving a single $\mathtt{alloc(x)}$ predicate from $\mathtt{alloc(x)} * \top$ (with forthcoming intermediate axiom $\mathbf{(I_{12}^*)}$). Alternatively, it would have been possible to include "big-step" axiom schemas that, given the two Boolean combinations of core formulae, derive the equivalent formula in one single derivation step (see e.g. [EIP19]). The main difference is that small-step axioms provide a simpler understanding of the key properties of the logic.

$(\mathbf{A_1^C})$ $\mathtt{x} = \mathtt{x}$	$(\mathbf{A_4^C})$ $\mathtt{x} \hookrightarrow \mathtt{y} \wedge \mathtt{x} \hookrightarrow \mathtt{z} \Rightarrow \mathtt{y} = \mathtt{z}$
$(\mathbf{A_2^C})$ $\varphi \wedge \mathtt{x} = \mathtt{y} \Rightarrow \varphi[\mathtt{y} \leftarrow \mathtt{x}]$	$(\mathbf{I_5^C})$ $\mathtt{size} \geqslant \beta{+}1 \Rightarrow \mathtt{size} \geqslant \beta$
$(\mathbf{A_3^C})$ $\mathtt{x} \hookrightarrow \mathtt{y} \Rightarrow \mathtt{alloc(x)}$	$(\mathbf{I_6^C})$ $\bigwedge_{\mathtt{x} \in \mathtt{X}} (\mathtt{alloc(x)} \wedge \bigwedge_{\mathtt{y} \in \mathtt{X} \setminus \{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow \mathtt{size} \geqslant \mathrm{card}(\mathtt{X})$

Figure 4: Proof system $\mathcal{H}_{\mathsf{C}}$ for Boolean combinations of core formulae.

4. A simple calculus for the core formulae

To axiomatise $\mathsf{SL}(*, -\!\!*)$, we start by introducing the proof system $\mathcal{H}_{\mathsf{C}}$ dedicated to Boolean combinations of core formulae, see Figure 4. As explained earlier, it also contains the axiom schemata and modus ponens for the propositional calculus. Moreover, the axioms whose name is of the form A_i^{C} are axioms that remain in the global system for $\mathsf{SL}(*, -\!\!*)$, whereas those named I_i^{C} are intermediate axioms that are removed when considering the axioms dealing with the separating connectives. As explained before, the intermediate axioms are handy to establish results about the axiomatisation of Boolean combinations of core formulae but are not needed when all the axioms and rules of $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ are considered.

In the axiom $(\mathbf{A_2^C})$, $\varphi[\mathtt{y} \leftarrow \mathtt{x}]$ stands for the formula obtained from φ by replacing with the variable $\mathtt{x}$ every occurrence of $\mathtt{y}$. Let (s, h) be a memory state. The axioms state that $=$ is an equivalence relation (first two axioms), $h(s(\mathtt{x})) = s(\mathtt{y})$ implies $s(\mathtt{x}) \in \mathrm{dom}(h)$ (axiom $(\mathbf{A_3^C})$) and that h is a (partial) function (axiom $(\mathbf{A_4^C})$). Furthermore, there are two intermediate axioms about size formulae: $(\mathbf{I_5^C})$ states that if $\mathrm{dom}(h)$ has at least $\beta{+}1$ elements, then it has at least β elements, whereas $(\mathbf{I_6^C})$ states instead that if there are β distinct memory cells corresponding to program variables, then indeed $\mathrm{dom}(h) \geqslant \beta$. It is easy to check that $\mathcal{H}_{\mathsf{C}}$ is sound (see also Lemma 3.1). In order to establish its completeness with respect to Boolean combinations of core formulae, we first show that $\mathcal{H}_{\mathsf{C}}$ is complete for a subclass of Boolean combinations of core formulae, namely for *core types* defined below. Then, we show that every formula in $\mathsf{Bool}(\mathsf{Core}(\mathtt{X}, \alpha))$ is provably equivalent to a disjunction of core types (Lemma 4.2).

Introduction to core types. Let $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$ and $\alpha \in \mathbb{N}^+$. We write $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$ to denote the set of *core types* defined by

$$\big\{\varphi \in \mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \alpha)) \,\big|\, \text{for all } \psi \in \mathsf{Core}(\mathtt{X}, \alpha),\ \{\psi \mid \neg\psi\} \subseteq_{\mathsf{Lt}} \varphi, \text{ and } (\psi \wedge \neg\psi) \not\subseteq_{\mathsf{Lt}} \varphi\big\}.$$

Note that if $\varphi \in \mathsf{CoreTypes}(\mathtt{X}, \alpha)$, then φ is a conjunction such that for every $\psi \in \mathsf{Core}(\mathtt{X}, \alpha)$, there is exactly one literal in φ built upon ψ.

Lemma 4.1 (Refutational completeness)**.** *Let $\varphi \in \mathsf{CoreTypes}(\mathtt{X}, \alpha)$, where $\alpha \geqslant \mathrm{card}(\mathtt{X})$. The formula $\neg\varphi$ is valid if and only if $\vdash_{\mathcal{H}_{\mathsf{C}}} \neg\varphi$.*

Proof. We show that φ is unsatisfiable if and only if $\vdash_{\mathcal{H}_{\mathsf{C}}} \neg\varphi$. The "only if" part follows from the soundness of $\mathcal{H}_{\mathsf{C}}$, so we prove the "if" part. Let $\varphi \in \mathsf{CoreTypes}(\mathtt{X}, \alpha)$ be such that $\not\vdash_{\mathcal{H}_{\mathsf{C}}} \varphi \Rightarrow \bot$, and let us prove that φ is satisfiable. By the axioms $(\mathbf{A_1^C})$ and $(\mathbf{A_2^C})$, there is an equivalence relation $\approx$ on $\mathtt{X}$ such that $\mathtt{x} \approx \mathtt{y}$ iff $\mathtt{x} = \mathtt{y}$ occurs positively in φ. We write $[\mathtt{x}]$ to denote the equivalence class of $\mathtt{x}$ with respect to $\approx$. By the axioms $(\mathbf{A_2^C})$ and $(\mathbf{A_4^C})$, there is a partial map $f : (\mathtt{X}/\approx) \to (\mathtt{X}/\approx)$ on equivalence classes such that $\mathtt{x} \hookrightarrow \mathtt{y}$ occurs positively iff $f([x])$ is defined and $f([x]) = [y]$. Let $D = \{[\mathtt{x}] \mid \mathtt{alloc(x)} \text{ occurs positively in } \varphi\}$. By the axiom $(\mathbf{A_3^C})$, $\mathsf{dom}(f) \subseteq D$. Let $n = \max_{\mathtt{size}}(\varphi)$. We recall that, by definition of $\max_{\mathtt{size}}(.)$, n is the greatest β such that $\mathtt{size} \geqslant \beta$ occurs positively in φ (or zero if there are none).

Let us show that $n \geqslant \mathrm{card}(D)$. *Ad absurdum*, suppose that $n < \mathrm{card}(D)$. From the axiom $\mathbf{(I_6^C)}$, $\vdash_{\mathcal{H}_\mathsf{C}} \varphi \Rightarrow \mathtt{size} \geqslant \mathrm{card}(D)$ and by definition of n and the fact that $\alpha \geqslant \mathrm{card}(\mathtt{X}) \geqslant \mathrm{card}(D)$, $\vdash_{\mathcal{H}_\mathsf{C}} \varphi \Rightarrow \mathtt{size} \geqslant n$ and $\vdash_{\mathcal{H}_\mathsf{C}} \varphi \Rightarrow \neg(\mathtt{size} \geqslant (n+1))$ since both $\mathtt{size} \geqslant n$ and $(\mathtt{size} \geqslant (n+1))$ (possibly negated) occur in φ as $\alpha \geqslant \mathrm{card}(\mathtt{X})$. By using the axiom $\mathbf{(I_5^C)}$ and propositional reasoning, we can get that $\vdash_{\mathcal{H}_\mathsf{C}} \varphi \Rightarrow \neg(\mathtt{size} \geqslant \mathrm{card}(D))$ since $\vdash_{\mathcal{H}_\mathsf{C}} \varphi \Rightarrow \neg(\mathtt{size} \geqslant (n+1))$, which leads to a contradiction. Consequently, $n \geqslant \mathrm{card}(D)$.

Let $\ell_0, \ell_1, \ldots, \ell_n \in \mathsf{LOC}$ be $n+1$ distinct locations, and let us fix an enumeration $C_1, \ldots, C_{\mathrm{card}(D)}$ on the equivalence classes of $\approx$. Let (s,h) be defined by

- $s(\mathtt{x}) \stackrel{\text{def}}{=} \ell_i$ if $[x]$ is the ith equivalence class C_i,
- $h(\ell_i) \stackrel{\text{def}}{=} \ell_j$ if $0 < i \leqslant \mathrm{card}(D)$ and the ith equivalence class is mapped to the jth one by f,
- $h(\ell_i) \stackrel{\text{def}}{=} \ell_0$ if either $0 < i \leqslant \mathrm{card}(D)$ and the ith equivalence class is not in the domain of f, or $i > \mathrm{card}(D)$.

Then, by construction, (s,h) satisfies all positive literals of the form $\mathtt{x} = \mathtt{y}$ or $\mathtt{x} \hookrightarrow \mathtt{y}$ or $\mathtt{alloc}(\mathtt{x})$ that occur positively in φ, and all negative literals that occur in φ. It also satisfies $\mathtt{size} \geqslant n$, falsifies $\mathtt{size} \geqslant n+1$ (assuming $n+1 \leqslant \alpha$), and by the axiom $\mathbf{(I_5^C)}$, it satisfies all size literals in φ. □

By classical reasoning, one can show that every $\varphi \in \mathsf{Bool}(\mathsf{Core}(\mathtt{X}, \alpha))$ is provably equivalent to a disjunction of core types. Together with Lemma 4.1, this implies that $\mathcal{H}_\mathsf{C}$ is adequate with respect to the propositional logic of core formulae.

To prove forthcoming Theorem 4.3, let us first establish the following simple lemma.

Lemma 4.2 (Core Types Lemma)**.** *Let $\varphi \in \mathsf{Bool}(\mathsf{Core}(\mathtt{X}, \alpha))$. There is a disjunction $\psi = \psi_1 \vee \ldots \vee \psi_n$ with $\psi_i \in \mathsf{CoreTypes}(\mathtt{X}, \max(\mathrm{card}(\mathtt{X}), \alpha))$ for all i such that $\vdash_{\mathcal{H}_\mathsf{C}} \varphi \Leftrightarrow \psi$.*

Proof. Let $\psi_1 \vee \ldots \vee \psi_n$ be a formula in disjunctive normal form logically equivalent to φ. If ψ_i is not a core type in $\mathsf{CoreTypes}(\mathtt{X}, \max(\mathrm{card}(\mathtt{X}), \alpha))$, there is a core formula $\chi \in \mathsf{Core}(\mathtt{X}, \max(\mathrm{card}(\mathtt{X}), \alpha))$ that occurs neither positively nor negatively in ψ_i. Replacing ψ_i with $(\psi_i \wedge \chi) \vee (\psi_i \wedge \neg\chi)$, and repeating this for all missing core formulae and for all i, we obtain a disjunction of core types of the expected form. Since all equivalences follow from pure propositional reasoning, the equivalence between φ and the obtained formula can be proved in $\mathcal{H}_\mathsf{C}$. □

Theorem 4.3 (Adequacy)**.** *A Boolean combination of core formulae φ is valid iff $\vdash_{\mathcal{H}_\mathsf{C}} \varphi$.*

Proof. Let φ be a Boolean combination of core formulae in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$ for some $\mathtt{X}$ and α. As all the axioms are valid (Lemma 3.1), $\vdash_{\mathcal{H}_\mathsf{C}} \varphi$ implies that φ is valid. Let us assume that φ is valid, and let us prove that $\vdash_{\mathcal{H}_\mathsf{C}} \varphi$. By Lemma 4.2, there is a disjunction $\psi = \psi_1 \vee \ldots \vee \psi_n$ of core types in $\mathsf{CoreTypes}(\mathtt{X}, \max(\mathrm{card}(\mathtt{X}), \alpha))$ such that $\vdash_{\mathcal{H}_\mathsf{C}} (\neg\varphi) \Leftrightarrow \psi$. As φ is valid, the formulae $\neg\varphi$, ψ and all the ψ_i's are unsatisfiable. By Lemma 4.1, $\vdash_{\mathcal{H}_\mathsf{C}} \psi_i \Rightarrow \bot$, for all i. By propositional reasoning, $\vdash_{\mathcal{H}_\mathsf{C}} \varphi$. □

5. Axiomatisation for $\mathsf{SL}(*, \mathtt{alloc})$

We write $\mathsf{SL}(*, \mathtt{alloc})$ to denote the fragment of $\mathsf{SL}(*, -\!\!*)$ in which the separating implication is removed at the price of adding the atomic formulae of the form $\mathtt{alloc}(\mathtt{x})$. We define an Hilbert-style axiomatisation for $\mathsf{SL}(*, \mathtt{alloc})$, obtained by enriching $\mathcal{H}_\mathsf{C}$ with axioms and one inference rule that handle the separating conjunction $*$, leading to the proof system $\mathcal{H}_\mathsf{C}(*)$.

$(\mathbf{A}^*_7)$ $(\varphi * \psi) \Leftrightarrow (\psi * \varphi)$

$(\mathbf{A}^*_8)$ $(\varphi * \psi) * \chi \Leftrightarrow \varphi * (\psi * \chi)$

$(\mathbf{I}^*_9)$ $(\varphi \vee \psi) * \chi \Rightarrow (\varphi * \chi) \vee (\psi * \chi)$

$(\mathbf{I}^*_{10})$ $(\bot * \varphi) \Leftrightarrow \bot$

$(\mathbf{A}^*_{11})$ $\varphi \Leftrightarrow \varphi * \mathtt{emp}$

$(\mathbf{I}^*_{12})$ $\mathtt{alloc(x)} * \top \Rightarrow \mathtt{alloc(x)}$

$(\mathbf{A}^*_{13})$ $(\mathtt{alloc(x)} * \mathtt{alloc(x)}) \Leftrightarrow \bot$

$(\mathbf{A}^*_{14})$ $\mathtt{e} * \top \Rightarrow \mathtt{e}$ $\quad [\mathtt{e} \in \{\neg\mathtt{emp},\ \mathtt{x} = \mathtt{y},\ \mathtt{x} \neq \mathtt{y},\ \mathtt{x} \hookrightarrow \mathtt{y}\}]$

$(\mathbf{A}^*_{15})$ $\neg\mathtt{alloc(x)} * \neg\mathtt{alloc(x)} \Rightarrow \neg\mathtt{alloc(x)}$

$(\mathbf{A}^*_{16})$ $(\mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}) * \top \Rightarrow \neg\mathtt{x} \hookrightarrow \mathtt{y}$

$(\mathbf{A}^*_{17})$ $\mathtt{alloc(x)} \Rightarrow (\mathtt{alloc(x)} \wedge \mathtt{size} = 1) * \top$

$(\mathbf{A}^*_{18})$ $\neg\mathtt{emp} \Rightarrow \mathtt{size} = 1 * \top$

$(\mathbf{A}^*_{19})$ $\neg\mathtt{size} \geqslant \beta_1 * \neg\mathtt{size} \geqslant \beta_2 \Rightarrow \neg\mathtt{size} \geqslant \beta_1 + \beta_2 \dot{-} 1$

$(\mathbf{A}^*_{20})$ $\mathtt{alloc(x)} \wedge \mathtt{alloc(y)} \wedge \mathtt{x} \neq \mathtt{y} \Rightarrow \mathtt{size} \geqslant 2$

$*$**-Intro**: $\dfrac{\varphi \Rightarrow \chi}{\varphi * \psi \Rightarrow \chi * \psi}$ $\qquad (a \dot{-} b = \max(0, a - b))$

Figure 5: Additional axioms and rule for $\mathcal{H}_{\mathsf{C}}(*)$.

Fundamentally, as we work now within $\mathsf{SL}(*, \mathtt{alloc})$, the core formula $\mathtt{size} \geqslant \beta$ can be encoded in the logic. According to its definition, given in Section 2.2, we see $\mathtt{size} \geqslant 0$ as $\top$, $\mathtt{size} \geqslant 1$ as $\neg\mathtt{emp}$ and $\mathtt{size} \geqslant \beta{+}2$ as $\neg\mathtt{emp} * \mathtt{size} \geqslant \beta{+}1$.

The axioms and the rule added to $\mathcal{H}_{\mathsf{C}}$ in order to define $\mathcal{H}_{\mathsf{C}}(*)$ are presented in Figure 5. Their soundness has been proved in Lemma 3.1, with the exception of the three intermediate axioms $\mathbf{(I^*_9)}$, $\mathbf{(I^*_{10})}$ and $\mathbf{(I^*_{12})}$, which are used for the completeness of $\mathcal{H}_{\mathsf{C}}(*)$ with respect to $\mathsf{SL}(*, \mathtt{alloc})$, but are discharged from the proof system for $\mathsf{SL}(*, -\!\!*)$ (Figure 1), as they become derivable (Lemma 6.1).

Lemma 5.1. *$\mathcal{H}_{\mathsf{C}}(*)$ is sound.*

Proof. The axioms $\mathbf{(I^*_9)}$ and $\mathbf{(I^*_{10})}$ are inherited from Boolean BI (see [BV14] and [GLW06, Section 2]). The soundness of $\mathbf{(I^*_{12})}$ is straightforward. Indeed, suppose $(s, h) \models \mathtt{alloc(x)} * \top$. So, there is $h' \sqsubseteq h$ such that $(s, h') \models \mathtt{alloc(x)}$. By definition of $\mathtt{alloc(x)}$, $s(\mathtt{x}) \in \mathrm{dom}(h')$. By $h' \sqsubseteq h$, $s(\mathtt{x}) \in \mathrm{dom}(h)$. We conclude that $(s, h) \models \mathtt{alloc(x)}$. □

Let us look further at the axioms in Figure 5. The axioms deal with the commutative monoid properties of $(*, \mathtt{emp})$ and its distributivity over $\vee$ (as for Boolean BI, see e.g. [GLW06]). The rule $*$**-Intro**, sometimes called "frame rule" by analogy with the rule of the same name in program logic, states that logical equivalence is a congruence for $*$. $\mathcal{H}_{\mathsf{C}}(*)$ is designed with the idea of being as simple as possible. On one side, this helps understanding the key ingredients of $\mathsf{SL}(*, \mathtt{alloc})$. On the other side, this makes the proof of completeness of $\mathcal{H}_{\mathsf{C}}(*)$ more challenging. To work towards this proof while familiarising with the new axioms, we first show a set of intermediate theorems (see Appendix A).

Lemma 5.2. *The following rules and axioms are admissible in $\mathcal{H}_{\mathsf{C}}(*)$:*

$\mathbf{(I^*_{5.2.1})}$ $\mathtt{x} \sim \mathtt{y} \wedge (\varphi * \psi) \Rightarrow (\varphi \wedge \mathtt{x} \sim \mathtt{y}) * \psi$, *where $\sim$ stands for $=$ or $\neq$.*

$\mathbf{(I^*_{5.2.2})}$ $\mathtt{x} = \mathtt{y} \wedge ((\varphi \wedge \mathtt{alloc(x)}) * \psi) \Rightarrow (\varphi \wedge \mathtt{alloc(y)}) * \psi$.

$\mathbf{(I^*_{5.2.3})}$ $(\varphi \wedge \mathtt{alloc(x)}) * \psi \Rightarrow \varphi * (\psi \wedge \neg\mathtt{alloc(x)})$.

$\mathbf{(I^*_{5.2.4})}$ $\neg\mathtt{alloc(x)} \wedge (\varphi * \psi) \Rightarrow (\varphi \wedge \neg\mathtt{alloc(x)}) * \psi$.

$\mathbf{(I^*_{5.2.5})}$ $\mathtt{alloc(x)} \wedge (\varphi * (\neg\mathtt{alloc(x)} \wedge \psi)) \Rightarrow (\varphi \wedge \mathtt{alloc(x)}) * (\neg\mathtt{alloc(x)} \wedge \psi)$

$\mathbf{(I^*_{5.2.6})}$ $\mathtt{x} \hookrightarrow \mathtt{y} \wedge ((\varphi \wedge \mathtt{alloc(x)}) * \psi) \Rightarrow (\varphi \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi$.

$\mathbf{(I^*_{5.2.7})}$ $\neg\mathtt{x} \hookrightarrow \mathtt{y} \wedge (\varphi * \psi) \Rightarrow (\varphi \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}) * \psi$.

In $\mathcal{H}_{\mathsf{C}}(*)$, the axioms $\mathbf{(I_5^C)}$ and $\mathbf{(I_6^C)}$ of $\mathcal{H}_{\mathsf{C}}$ are superfluous and can be removed. Indeed, notice that both axioms do not appear in the proof system $\mathcal{H}_{\mathsf{C}}(*,-\!\!*)$ given in Figure 1.

Lemma 5.3. *The axioms* $\mathbf{(I_5^C)}$ *and* $\mathbf{(I_6^C)}$ *are derivable in* $\mathcal{H}_{\mathsf{C}}(*)$.

Validity of $\mathbf{(I_5^C)}$. The proof is by induction on β.

base case: $\beta = 0$**:** The instance of the axiom $\mathbf{(I_5^C)}$ with $\beta = 0$ amounts to derive the formula $\mathtt{size} \geqslant 1 \Rightarrow \mathtt{size} \geqslant 0$. By definition $\mathtt{size} \geqslant 1 = \neg\mathtt{emp}$ and $\mathtt{size} \geqslant 0 = \top$, and therefore, by propositional reasoning, $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathtt{size} \geqslant 1 \Rightarrow \mathtt{size} \geqslant 0$.

induction step: $\beta > 0$**:** By induction hypothesis, assume $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathtt{size} \geqslant \beta \Rightarrow \mathtt{size} \geqslant \beta - 1$. The formula $\mathtt{size} \geqslant \beta + 1 \Rightarrow \mathtt{size} \geqslant \beta$ is derived as follows:

1	$\mathtt{size} \geqslant \beta \Rightarrow \mathtt{size} \geqslant \beta - 1$	Induction hypothesis
2	$(\mathtt{size} \geqslant \beta) * \neg\mathtt{emp} \Rightarrow (\mathtt{size} \geqslant \beta - 1) * \neg\mathtt{emp}$	$*$**-Intro**, 1
3	$\mathtt{size} \geqslant \beta + 1 \Rightarrow \mathtt{size} \geqslant \beta$	2, def. of $\mathtt{size}$ $\square$

Before proving the validity of $\mathbf{(I_6^C)}$, we derive the intermediate theorem below. Let $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$.

$\mathbf{(I_{5.3.1}^{-\!*})}$ $\bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow (\divideontimes_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \mathtt{size} = 1)) * \top$.

Validity of $\mathbf{(I_{5.3.1}^{-\!*})}$. The proof is by induction on the size of $\mathtt{X}$. We distinguish two base cases, for $\mathrm{card}(\mathtt{X}) = 1$ and $\mathrm{card}(\mathtt{X}) = 0$.

base case: $\mathrm{card}(\mathtt{X}) = 1$**:** In this case, $\mathbf{(I_{5.3.1}^{-\!*})}$ is exactly $\mathbf{(A_{17}^*)}$.

base case: $\mathrm{card}(\mathtt{X}) = 0$**:** In this case, $\mathbf{(I_{5.3.1}^{-\!*})}$ is $\top \Rightarrow \top * \top$.

1	$\mathtt{emp} \Rightarrow \top$	PC
2	$\top \Rightarrow \top * \mathtt{emp}$	$\mathbf{(A_{11}^*)}$
3	$\top * \mathtt{emp} \Rightarrow \mathtt{emp} * \top$	$\mathbf{(A_7^*)}$
4	$\mathtt{emp} * \top \Rightarrow \top * \top$	$*$**-Intro**, 1
5	$\top \Rightarrow \top * \top$	$\Rightarrow$**-Tr**, 2, 3, 4

induction step: $\mathrm{card}(\mathtt{X}) \geqslant 2$**:** Let $\mathtt{z} \in \mathtt{X}$. By induction hypothesis,

$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \bigwedge_{\mathtt{u}\in\mathtt{X}\setminus\{\mathtt{z}\}}(\mathtt{alloc}(\mathtt{u}) \wedge \bigwedge_{\mathtt{v}\in\mathtt{X}\setminus\{\mathtt{u},\mathtt{z}\}} \mathtt{u} \neq \mathtt{v}) \Rightarrow (\divideontimes_{\mathtt{u}\in\mathtt{X}\setminus\{\mathtt{z}\}}(\mathtt{alloc}(\mathtt{u}) \wedge \mathtt{size} = 1)) * \top$.

We write χ for the premise $\bigwedge_{\mathtt{u}\in\mathtt{X}\setminus\{\mathtt{z}\}}(\mathtt{alloc}(\mathtt{u}) \wedge \bigwedge_{\mathtt{v}\in\mathtt{X}\setminus\{\mathtt{u},\mathtt{z}\}} \mathtt{u} \neq \mathtt{v})$ above. Below, we aim for a proof of

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow (\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \chi.$$

In this way, the provability of $\mathbf{(I_{5.3.1}^{-\!*})}$ follows directly by induction hypothesis together with $\mathbf{(A_7^*)}$ and $*$**-Intro**. We have

1	$\bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow (\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \top$	$\mathbf{(A_{17}^*)}$ and PC
2	$\top \Rightarrow \chi \vee \neg\chi$	PC
3	$(\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \top \Rightarrow (\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * (\chi \vee \neg\chi)$	$*$**-Intro**, $\mathbf{(A_7^*)}$, 2
4	$(\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * (\chi \vee \neg\chi) \Rightarrow$	

	$((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \chi) \vee ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \neg\chi)$	$\mathbf{(A_7^*)}$ and $\mathbf{(I_9^*)}$
5	$\bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow$	
	$((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \chi) \vee ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \neg\chi)$	$\Rightarrow$**-Tr** 1, 3, 4

By propositional reasoning, $\neg\chi$ is equivalent to $\bigvee_{\mathtt{u}\in\mathtt{X}\setminus\{\mathtt{z}\}}(\neg\mathtt{alloc}(\mathtt{u}) \vee \bigvee_{\mathtt{v}\in\mathtt{X}\setminus\{\mathtt{u},\mathtt{z}\}} \mathtt{u} = \mathtt{v})$. Due to the complexity of this formula, we proceed now rather informally, but our arguments entail the existence of a proper derivation. We aim at showing that

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \wedge ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \neg\chi) \Rightarrow \bot\,. \qquad (\dagger)$$

By propositional calculus and $\mathbf{(I_9^*)}$, we can distribute conjunctions and separating conjunctions over disjunctions. We derive:

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \wedge ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \neg\chi) \Rightarrow \gamma' \vee \gamma'',$$

where γ' and γ'' are defined, respectively, as

$$\bigvee_{\mathtt{u}\in\mathtt{X}\setminus\{\mathtt{z}\}}\Big(\bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \wedge ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \neg\mathtt{alloc}(\mathtt{u}))\Big)\,,$$

$$\bigvee_{\substack{\mathtt{u}\in\mathtt{X}\setminus\{\mathtt{z}\}\\ \mathtt{v}\in\mathtt{X}\setminus\{\mathtt{z},\mathtt{u}\}}}\Big(\bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \wedge ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \mathtt{u} = \mathtt{v})\Big).$$

In order to deduce (†) it is sufficient to prove, in $\mathcal{H}_{\mathsf{C}}(*)$, that every disjunct of γ' and γ'' implies $\bot$. Clearly, if γ' and γ'' do not have any disjunct, i.e. when $\mathtt{X}\setminus\{\mathtt{z}\}$ is empty, then the formula is propositionally equivalent to $\bot$, which allows us to conclude (†). Otherwise, let us consider each disjunct in γ' and γ'' (separately), and prove their inconsistency.
case: γ': Let $\mathtt{u} \in \mathtt{X}\setminus\{\mathtt{z}\}$. We show the inconsistency of

$$\overline{\gamma} \stackrel{\text{def}}{=} \bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \wedge ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \neg\mathtt{alloc}(\mathtt{u})).$$

6	$\bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\setminus\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow \mathtt{alloc}(\mathtt{u}) \wedge \mathtt{u} \neq \mathtt{z}$	PC
7	$\overline{\gamma} \Rightarrow \mathtt{alloc}(\mathtt{u}) \wedge \mathtt{u} \neq \mathtt{z} \wedge ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \neg\mathtt{alloc}(\mathtt{u}))$	PC
8	$\mathtt{alloc}(\mathtt{u}) \wedge ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \neg\mathtt{alloc}(\mathtt{u})) \Rightarrow$ $((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1 \wedge \mathtt{alloc}(\mathtt{u})) * \neg\mathtt{alloc}(\mathtt{u}))$	$\mathbf{(I_{5.2.5}^*)}$
9	$\mathtt{u} \neq \mathtt{z} \wedge ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1 \wedge \mathtt{alloc}(\mathtt{u})) * \neg\mathtt{alloc}(\mathtt{u})) \Rightarrow$ $((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1 \wedge \mathtt{alloc}(\mathtt{u}) \wedge \mathtt{u} \neq \mathtt{z}) * \neg\mathtt{alloc}(\mathtt{u}))$	$\mathbf{(I_{5.2.1}^*)}$
10	$\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{alloc}(\mathtt{u}) \wedge \mathtt{u} \neq \mathtt{z} \Rightarrow \mathtt{size} \geqslant 2$	$\mathbf{(A_{20}^*)}$
11	$\mathtt{size} = 1 \Rightarrow \neg\mathtt{size} \geqslant 2$	PC
12	$\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1 \wedge \mathtt{alloc}(\mathtt{u}) \wedge \mathtt{u} \neq \mathtt{z} \Rightarrow \bot$	$\Rightarrow$**-Tr**, PC, 10, 11
13	$\overline{\gamma} \Rightarrow (\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1 \wedge \mathtt{alloc}(\mathtt{u}) \wedge \mathtt{u} \neq \mathtt{z}) * \neg\mathtt{alloc}(\mathtt{u})$	PC, 7, 8, 9
14	$(\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1 \wedge \mathtt{alloc}(\mathtt{u}) \wedge \mathtt{u} \neq \mathtt{z}) * \neg\mathtt{alloc}(\mathtt{u}) \Rightarrow \bot * \neg\mathtt{alloc}(\mathtt{u})$	$*$**-Intro**, 12
15	$\bot * \neg\mathtt{alloc}(\mathtt{u}) \Rightarrow \bot$	$\mathbf{(I_{10}^*)}$, 14
16	$\overline{\gamma} \Rightarrow \bot$	PC, 13, 15

Since $\overline{\gamma}$ is an arbitrary disjunct appearing in γ', we conclude that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \gamma' \Rightarrow \bot$.

case: γ'': Let $\mathtt{u} \in \mathtt{X}\backslash\{\mathtt{z}\}$ and $\mathtt{v} \in \mathtt{X}\backslash\{\mathtt{z},\mathtt{u}\}$. Notice that if $\mathtt{u}$ or $\mathtt{v}$ do not exist, then γ'' is defined as $\bot$ and so the proof is complete. Otherwise, we show the inconsistency of

$$\widehat{\gamma} \stackrel{\text{def}}{=} \bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\backslash\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \wedge ((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \mathtt{u} = \mathtt{v}).$$

17	$\bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\backslash\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow \mathtt{u} \neq \mathtt{v}$	PC
18	$\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1 \Rightarrow \top$	PC
19	$(\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \mathtt{u} = \mathtt{v} \Rightarrow \mathtt{u} = \mathtt{v} * \top$	$*$**-Intro**, 18, $\mathbf{(A_7^*)}$
20	$\mathtt{u} = \mathtt{v} * \top \Rightarrow \mathtt{u} = \mathtt{v}$	$\mathbf{(A_{14}^*)}$
21	$((\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \mathtt{u} = \mathtt{v}) \Rightarrow \mathtt{u} = \mathtt{v}$	$\Rightarrow$**-Tr**, 19, 20
22	$\widehat{\gamma} \Rightarrow \bot$	PC, 17, 21

Since $\widehat{\gamma}$ is an arbitrary disjunct appearing in γ'', we conclude that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \gamma'' \Rightarrow \bot$. From $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \gamma' \Rightarrow \bot$ and $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \gamma'' \Rightarrow \bot$ we conclude that (†) holds. From the theorem 5 derived in this proof, this allows us to conclude that

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\backslash\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow (\mathtt{alloc}(\mathtt{z}) \wedge \mathtt{size} = 1) * \chi,$$

which concludes the proof, as explained at the beginning of the induction step. □

We complete the proof of Lemma 5.3 by showing a derivation of $\mathbf{(I_6^C)}$.

Validity of $\mathbf{(I_6^C)}$. Let $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$. If $\mathtt{X} = \varnothing$, then the instance of the axiom $\mathbf{(I_6^C)}$ becomes $\top \Rightarrow \mathtt{size} \geqslant 0$, which, by definition of $\mathtt{size} \geqslant 0$, is syntactically equivalent to $\top \Rightarrow \top$ and hence valid by propositional reasoning. Below, assume $\mathtt{X} \neq \varnothing$ and fix $\mathtt{z} \in \mathtt{X}$.

1	$\bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\backslash\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow$ $(\circledast_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \mathtt{size} = 1)) * \top$	$\mathbf{(I_{5.3.1}^{-*})}$
2	$\mathtt{alloc}(\mathtt{x}) \wedge \mathtt{size} = 1 \Rightarrow \mathtt{size} \geqslant 1$	PC, def. of $\mathtt{size} = 1$
3	$(\circledast_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \mathtt{size} = 1)) * \top \Rightarrow (\circledast_{\mathtt{x}\in\mathtt{X}}\mathtt{size} \geqslant 1) * \top$	multiple applications of $*$**-Intro**, 2, $\mathbf{(A_7^*)}$ and $\Rightarrow$**-Tr**
4	$(\circledast_{\mathtt{x}\in\mathtt{X}}\mathtt{size} \geqslant 1) * \top \Rightarrow (\mathtt{size} \geqslant 1 * \top) * (\circledast_{\mathtt{x}\in\mathtt{X}\backslash\{\mathtt{z}\}}\mathtt{size} \geqslant 1)$	$\mathbf{(A_7^*)}$, $\mathbf{(A_8^*)}$, def. of $\mathtt{z}$
5	$\mathtt{size} \geqslant 1 * \top \Rightarrow \mathtt{size} \geqslant 1$	$\mathbf{(A_{14}^*)}$, def. of $\mathtt{size} \geqslant 1$
6	$(\mathtt{size} \geqslant 1 * \top) * (\circledast_{\mathtt{x}\in\mathtt{X}\backslash\{\mathtt{z}\}}\mathtt{size} \geqslant 1) \Rightarrow (\circledast_{\mathtt{x}\in\mathtt{X}}\mathtt{size} \geqslant 1)$	$*$**-Intro**
7	$(\circledast_{\mathtt{x}\in\mathtt{X}}\mathtt{size} \geqslant 1) \Rightarrow \mathtt{size} \geqslant \mathrm{card}(\mathtt{X})$	$\mathbf{(A_8^*)}$, def. of $\mathtt{size} \geqslant \mathrm{card}(\mathtt{X})$
8	$\bigwedge_{\mathtt{x}\in\mathtt{X}}(\mathtt{alloc}(\mathtt{x}) \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}\backslash\{\mathtt{x}\}} \mathtt{x} \neq \mathtt{y}) \Rightarrow \mathtt{size} \geqslant \mathrm{card}(\mathtt{X})$	$\Rightarrow$**-Tr**, 1, 3, 4, 6, 7 □

From now on, we understand $\mathcal{H}_{\mathsf{C}}(*)$ as the proof system obtained from $\mathcal{H}_{\mathsf{C}}$ by adding all schemata from Figure 5 but by removing $\mathbf{(I_5^C)}$ and $\mathbf{(I_6^C)}$. We show that $\mathcal{H}_{\mathsf{C}}(*)$ enjoys the $*$ elimination property when the argument formulae are core types. That is, given two satisfiable core types φ and ψ, in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, we show that the formula $\varphi * \psi$ is provably equivalent to the formula $\langle * \rangle(\varphi, \psi)$ in $\mathsf{Conj}(\mathsf{Core}(\mathtt{X}, 2\alpha))$, defined in Figure 6.

$$\bigwedge \big\{ \mathtt{x} \sim \mathtt{y} \subseteq_{\mathsf{Lt}} \{\varphi \mid \psi\} \,\big|\, {\sim} \in \{=, \neq\} \big\} \quad \wedge \bigwedge \{ \mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \{\varphi \mid \psi\} \}$$
$$\wedge \bigwedge \{ \neg\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \{\varphi \,;\, \psi\} \} \quad \wedge \bigwedge \big\{ \neg\mathtt{x} \hookrightarrow \mathtt{y} \,\big|\, \mathtt{alloc}(\mathtt{x}) \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \{\varphi \mid \psi\} \big\}$$
$$\wedge \bigwedge \big\{ \mathtt{x} \neq \mathtt{x} \,\big|\, \mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \{\varphi \,;\, \psi\} \big\} \quad \wedge \bigwedge \left\{ \mathtt{size} \geqslant \beta_1{+}\beta_2 \,\middle|\, \begin{array}{l} \mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi \\ \mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$
$$\wedge \bigwedge \{ \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \{\varphi \mid \psi\} \} \quad \wedge \bigwedge \left\{ \neg\mathtt{size} \geqslant \beta_1{+}\beta_2{\dot{-}}1 \,\middle|\, \begin{array}{l} \neg\mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi \\ \neg\mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$

Figure 6: The formula $\langle * \rangle(\varphi, \psi)$.

Lemma 5.4. *Let* $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$ *and* $\alpha \geqslant \mathrm{card}(\mathtt{X})$*. If* φ *and* ψ *are two satisfiable core types in* $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$*, then* $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi * \psi \Leftrightarrow \langle * \rangle(\varphi, \psi)$*.*

The equivalence $\varphi * \psi \Leftrightarrow \langle * \rangle(\varphi, \psi)$ is reminiscent to the one in [EIP19, Lemma 3] that is proved semantically. In a way, because $\mathcal{H}_{\mathsf{C}}(*)$ will reveal to be complete, the restriction of [EIP19, Lemma 3] to $\mathsf{SL}(*, \mathtt{alloc})$ can be replayed completely syntactically within $\mathcal{H}_{\mathsf{C}}(*)$.

Structure of the proof of Lemma 5.4. Before presenting the technical developments, let us explain the structure of the whole proof of Lemma 5.4, which might help to follow the different steps. In order to show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi * \psi \Leftrightarrow \langle * \rangle(\varphi, \psi)$, we start showing that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi * \psi \Rightarrow \langle * \rangle(\varphi, \psi)$. This can be done rather mechanically since for every literal L of $\langle * \rangle(\varphi, \psi)$, one can construct a derivation for $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi * \psi \Rightarrow L$. The main difficulty in the proof rests on showing that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi * \psi$. To do so, we build a sequence of formulae $\varphi^{(1)} * \psi^{(1)}$, $\varphi^{(2)} * \psi^{(2)}$, …, $\varphi^{(k)} * \psi^{(k)}$ satisfying the following conditions:

- for all $i \in [1, k]$, $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$, the formulae $\varphi^{(i)}$ and $\psi^{(i)}$ are conjunctions of core formulae, and
- for all $j \in [1, i]$, $\varphi^{(j)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$ and $\psi^{(j)} \subseteq_{\mathsf{Lt}} \psi^{(i)}$.
- $\varphi = \varphi^{(k)}$ and $\psi = \psi^{(k)}$ (modulo associativity/commutativity of the classical conjunction).

In order to build φ^{i+1} (resp. ψ^{i+1}), we identify a literal L in φ (resp. in ψ) that does not occur yet in φ^i and we show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i+1)} * \psi^{(i+1)}$ with $\varphi^{i+1} \stackrel{\text{def}}{=} \varphi^{(i)} \wedge L$ (resp. $\psi^{(i+1)} \stackrel{\text{def}}{=} \psi^{(i)} \wedge L$) and $\psi^{(i+1)} \stackrel{\text{def}}{=} \psi^{(i)}$ (resp. $\varphi^{(i+1)} \stackrel{\text{def}}{=} \varphi^{(i)}$). The case analysis on the shape of the literal L is rather mechanical but it remains to specify how the first formulae $\varphi^{(1)}$ and $\psi^{(1)}$ are designed. In short, $\varphi^{(1)}$ (resp. $\psi^{(1)}$) is dedicated to the part of φ (resp. ψ) related to the size of the heap domain and to the allocated variables. Details will follow.

To construct these above-mentioned derivations, some additional derivations are instrumental in particular to establish that the formulae below are derivable in $\mathcal{H}_{\mathsf{C}}(*)$:

$$\mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} \geqslant \beta_2, \qquad \mathtt{size} = \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} = \beta_2.$$

Such derivations can be found in Appendix B. We now develop the proof of Lemma 5.4.

Proof of Lemma 5.4. First of all, let us briefly explain what is the rationale for having literals of the form $\mathtt{x} \neq \mathtt{x}$ in the definition of $\langle * \rangle(\varphi, \psi)$. Recall that $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \{\varphi \,;\, \psi\}$ is a shortcut to state that $\mathtt{alloc}(\mathtt{x})$ occurs in both the core types φ and ψ. Since $(\mathtt{alloc}(\mathtt{x}) \wedge \varphi') * (\mathtt{alloc}(\mathtt{x}) \wedge \psi')$ is unsatisfiable, $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \{\varphi \,;\, \psi\}$ entails that $\langle * \rangle(\varphi, \psi)$ should be unsatisfiable. That is why, if $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \{\varphi \,;\, \psi\}$, then $\mathtt{x} \neq \mathtt{x}$ is part of $\langle * \rangle(\varphi, \psi)$.

($\Rightarrow$): Let us show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi * \psi \Rightarrow \langle * \rangle(\varphi, \psi)$. We establish that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi * \psi \Rightarrow L$ holds for every literal L of $\langle * \rangle(\varphi, \psi)$. We reason by a case analysis on $L \subseteq_{\mathsf{Lt}} \langle * \rangle(\varphi, \psi)$.

case: L is an (in)equality or $L = \mathtt{x} \hookrightarrow \mathtt{y}$: For all the equalities and inequalities in φ or ψ, as well as all the literals of the form $\mathtt{x} \hookrightarrow \mathtt{y}$, $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi * \psi \Rightarrow L$ follows from the rule **$*$-Intro** and the axiom $\mathbf{(A^*_{14})}$. Let us provide below the proper derivation when L is a literal in φ that is an equality, an inequality or of the form $\mathtt{x} \hookrightarrow \mathtt{y}$.

1	$\varphi \Rightarrow L$	PC	4	$L * \top \Rightarrow L$	$\mathbf{(A^*_{14})}$
2	$\psi \Rightarrow \top$	PC	5	$\varphi * \psi \Rightarrow L$	$\Rightarrow$**-Tr**, 3, 4
3	$\varphi * \psi \Rightarrow L * \top$	$*$**-Ilr**, 1, 2			

Assume there is a literal $\mathtt{x} \neq \mathtt{x}$ that occurs in $\langle * \rangle(\varphi, \psi)$. As both φ and ψ are satisfiable, and thanks to $\mathbf{(A^{\mathsf{C}}_1)}$, this is necessarily due to $\mathtt{alloc(x)}$ occurring both in φ and ψ.

1	$\varphi \Rightarrow \mathtt{alloc(x)}$	PC	4	$\mathtt{alloc(x)} * \mathtt{alloc(x)} \Rightarrow \bot$	$\mathbf{(A^*_{13})}$
2	$\psi \Rightarrow \mathtt{alloc(x)}$	PC	5	$\bot \Rightarrow \mathtt{x} \neq \mathtt{x}$	PC
3	$\varphi * \psi \Rightarrow \mathtt{alloc(x)} * \mathtt{alloc(x)}$	$*$**-Ilr**, 1, 2	6	$\varphi * \psi \Rightarrow \mathtt{x} \neq \mathtt{x}$	$\Rightarrow$**-Tr**, 4, 5

case: $L = \mathtt{alloc(x)}$: Follows from $\mathbf{(I^*_{12})}$ and **$*$-Intro**.
case: $L = \neg\mathtt{alloc(x)}$: Follows from $\mathbf{(A^*_{15})}$ and **$*$-Intro**.
case: $L = \neg\mathtt{x} \hookrightarrow \mathtt{y}$: Let $\neg\mathtt{x} \hookrightarrow \mathtt{y}$ be a literal occurring in $\langle * \rangle(\varphi, \psi)$. So, $\mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}$ occurs in φ or ψ, say in φ (the other case is equivalent, due to $\mathbf{(A^*_7)}$).

1	$\varphi \Rightarrow \mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}$	PC
2	$\psi \Rightarrow \top$	PC
3	$\varphi * \psi \Rightarrow (\mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}) * \top$	$*$**-Ilr**, 1, 2
4	$(\mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}) * \top \Rightarrow \neg\mathtt{x} \hookrightarrow \mathtt{y}$	$\mathbf{(A^*_{16})}$
5	$\varphi * \psi \Rightarrow \neg\mathtt{x} \hookrightarrow \mathtt{y}$	$\Rightarrow$**-Tr**, 3, 4

case : $L = \mathtt{size} \geqslant \beta_1 + \beta_2$, where $\mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi$ and $\mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi$:

1	$\varphi \Rightarrow \mathtt{size} \geqslant \beta_1$	PC	3	$\varphi * \psi \Rightarrow \mathtt{size} \geqslant \beta_1 * \mathtt{size} \geqslant \beta_2$	$*$**-Ilr**, 1, 2
2	$\psi \Rightarrow \mathtt{size} \geqslant \beta_2$	PC	4	$\varphi * \psi \Rightarrow \mathtt{size} \geqslant (\beta_1 + \beta_2)$	Def. $\mathtt{size}$

Notice that, as φ and ψ are satisfiable core types, $\mathtt{size} \geqslant 0$ appears positively in both these formulae, and thus appears in $\langle * \rangle(\varphi, \psi)$.
case: $L = \neg\mathtt{size} \geqslant \beta_1 + \beta_2 \dot{-} 1$, where $\neg\mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi$ and $\neg\mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi$:

1	$\varphi \Rightarrow \neg\mathtt{size} \geqslant \beta_1$	PC
2	$\psi \Rightarrow \neg\mathtt{size} \geqslant \beta_2$	PC
3	$\varphi * \psi \Rightarrow \neg\mathtt{size} \geqslant \beta_1 * \neg\mathtt{size} \geqslant \beta_2$	$*$**-Ilr**, 1, 2
4	$\neg\mathtt{size} \geqslant \beta_1 * \neg\mathtt{size} \geqslant \beta_2 \Rightarrow \neg\mathtt{size} \geqslant \beta_1 + \beta_2 \dot{-} 1$	$\mathbf{(A^*_{19})}$
5	$\varphi * \psi \Rightarrow \neg\mathtt{size} \geqslant \beta_1 + \beta_2 \dot{-} 1$	$\Rightarrow$**-Tr**, 3, 4

($\Leftarrow$): Let us show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi * \psi$. If $\langle * \rangle(\varphi, \psi)$ is unsatisfiable, then by completeness of $\mathcal{H}_{\mathsf{C}}$ (Theorem 4.3), $\vdash_{\mathcal{H}_{\mathsf{C}}} \langle * \rangle(\varphi, \psi) \Rightarrow \bot$, and thus $\vdash_{\mathcal{H}_{\mathsf{C}}} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi * \psi$. Since $\mathcal{H}_{\mathsf{C}}(*)$ includes $\mathcal{H}_{\mathsf{C}}$, we conclude that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi * \psi$. Otherwise, below, we assume $\langle * \rangle(\varphi, \psi)$ to be satisfiable. In particular, this implies that no literals of the form $\mathtt{x} \neq \mathtt{x}$ or $\neg\mathtt{size} \geqslant 0$ appear in $\langle * \rangle(\varphi, \psi)$. Moreover, by definition of $\langle * \rangle(\varphi, \psi)$, this implies that φ, ψ and $\langle * \rangle(\varphi, \psi)$ agree on the satisfaction of the core formulae $\mathtt{x} = \mathtt{y}$, i.e. φ, ψ and $\langle * \rangle(\varphi, \psi)$ contain exactly the same (in)equalities. Since φ is satisfiable, these equalities define an equivalence relation. Let $\mathtt{x}_1, \ldots \mathtt{x}_n$ be a maximal enumeration of representatives of the equivalence classes (one per equivalence class) such that $\mathtt{alloc}(\mathtt{x}_i)$ occurs in $\langle * \rangle(\varphi, \psi)$. As it is maximal, for every $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \langle * \rangle(\varphi, \psi)$ there is $i \in [1, n]$ such that $\mathtt{x}_i$ is syntactically equal to $\mathtt{x}$. Consequently, from the definition of $\langle * \rangle(\varphi, \psi)$, if $\mathtt{alloc}(\mathtt{x})$ occurs in φ or in ψ, then there is some $\mathtt{x}_i$ such that $\mathtt{x} = \mathtt{x}_i$ occurs in φ (and therefore also in ψ and in $\langle * \rangle(\varphi, \psi)$). Let us define the formula *Alloc* below:

$$\mathit{Alloc} \stackrel{\text{def}}{=} \big(\mathtt{alloc}(\mathtt{x}_1) \wedge \mathtt{size} = 1\big) * \cdots * \big(\mathtt{alloc}(\mathtt{x}_n) \wedge \mathtt{size} = 1\big).$$

We have,

1	$\langle * \rangle(\varphi, \psi) \Rightarrow \bigwedge_{i \in [1,n]} (\mathtt{alloc}(\mathtt{x}_i) \wedge \bigwedge_{j \in [1,n] \setminus \{i\}} \mathtt{x}_i \neq \mathtt{x}_j)$	PC, def. of $\mathtt{x}_1, \ldots, \mathtt{x}_n$
2	$\bigwedge_{i \in [1,n]} (\mathtt{alloc}(\mathtt{x}_i) \wedge \bigwedge_{j \in [1,n] \setminus \{i\}} \mathtt{x}_i \neq \mathtt{x}_j) \Rightarrow \mathit{Alloc} * \top$	$\mathbf{(I^{-*}_{5.3.1})}$
3	$\langle * \rangle(\varphi, \psi) \Rightarrow \mathit{Alloc} * \top$	$\Rightarrow$**-Tr**, 1, 2

Moreover, we show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc} \Rightarrow \mathtt{size} \geqslant n$ and $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc} \Rightarrow \neg\mathtt{size} \geqslant n{+}1$ (theorems 4 and 7 below), and so $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc} \Rightarrow \mathtt{size} = n$.

1	$\chi \wedge \mathtt{size} = 1 \Rightarrow \mathtt{size} \geqslant 1$	PC, def. of $\mathtt{size} = 1$
2	$\chi \wedge \mathtt{size} = 1 \Rightarrow \neg\mathtt{size} \geqslant 2$	PC, def. of $\mathtt{size} = 1$
3	$\mathit{Alloc} \Rightarrow \circledast_{i \in [1,n]} \mathtt{size} \geqslant 1$	multiple applications of $*$**-Intro**, 1, $\mathbf{(A^*_7)}$ and $\Rightarrow$**-Tr**
4	$\mathit{Alloc} \Rightarrow \mathtt{size} \geqslant n$	3, def. of $\mathtt{size} \geqslant n$
5	$\mathit{Alloc} \Rightarrow \circledast_{i \in [1,n]} \neg\mathtt{size} \geqslant 2$	multiple applications of $*$**-Intro**, 2, $\mathbf{(A^*_7)}$ and $\Rightarrow$**-Tr**
6	$\circledast_{i \in [1,n]} \neg\mathtt{size} \geqslant 2 \Rightarrow \neg\mathtt{size} \geqslant n + 1$	n applications of $\mathbf{(A^*_{19})}$ and $*$**-Intro**
7	$\mathit{Alloc} \Rightarrow \neg\mathtt{size} \geqslant n + 1$	$\Rightarrow$**-Tr**, 5, 6
8	$\mathit{Alloc} \Rightarrow \mathtt{size} = n$	PC, 4, 7, def. of $\mathtt{size} = n$

After deriving $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \mathit{Alloc} * \top$ and $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc} \Rightarrow \mathtt{size} = n$, the proof is divided in three steps: (1) we isolate the allocated cells and the garbage, (2) we distribute the alloc and size literals according to the goal $\varphi * \psi$ and (3) we add the missing literals.

Step 1, isolating allocated cells and garbage. Since $\langle * \rangle(\varphi, \psi)$ is a conjunction of literals built from core formulae, we can rely on $\max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi))$, i.e. the maximum β among the formulae $\mathtt{size} \geqslant \beta$ appearing positively in $\langle * \rangle(\varphi, \psi)$. First, we show some important properties of $\langle * \rangle(\varphi, \psi)$, related to $\max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi))$.

A. $\max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi)) = \max_{\mathtt{size}}(\varphi) + \max_{\mathtt{size}}(\psi)$,

B. If there is $\beta \in \mathbb{N}$ such that $\neg\mathtt{size} \geqslant \beta \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi, \psi)$, then

$$\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathtt{Lt}} \varphi, \qquad \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\psi) + 1 \subseteq_{\mathtt{Lt}} \psi.$$

C. If there is $\beta \in \mathbb{N}$ such that $\neg\mathtt{size} \geqslant \beta \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi, \psi)$, then

$$\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi)) + 1 \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi, \psi).$$

Proof of (**A**). By definition of $\max_{\mathtt{size}}(.)$, we know that $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \subseteq_{\mathtt{Lt}} \varphi$ and $\mathtt{size} \geqslant \max_{\mathtt{size}}(\psi) \subseteq_{\mathtt{Lt}} \psi$. By definition of $\langle * \rangle(\varphi, \psi)$, $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + \max_{\mathtt{size}}(\psi) \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi, \psi)$. *Ad absurdum*, suppose that $\max_{\mathtt{size}}(\varphi) + \max_{\mathtt{size}}(\psi) \neq \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi))$ and thus, by definition of $\max_{\mathtt{size}}(.)$, there is $\beta > \max_{\mathtt{size}}(\varphi) + \max_{\mathtt{size}}(\psi)$ such that $\mathtt{size} \geqslant \beta \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi, \psi)$. By definition of $\langle * \rangle(\varphi, \psi)$, we conclude that there are β_1 and β_2 such that $\beta_1 + \beta_2 = \beta$, $\mathtt{size} \geqslant \beta_1 \subseteq_{\mathtt{Lt}} \varphi$ and $\mathtt{size} \geqslant \beta_2 \subseteq_{\mathtt{Lt}} \psi$. As $\beta_1 + \beta_2 > \max_{\mathtt{size}}(\varphi) + \max_{\mathtt{size}}(\psi)$, either $\beta_1 > \max_{\mathtt{size}}(\varphi)$ or $\beta_2 > \max_{\mathtt{size}}(\psi)$. Let us assume $\beta_1 > \max_{\mathtt{size}}(\varphi)$ (the other case is analogous). We have $\mathtt{size} \geqslant \beta_1 \subseteq_{\mathtt{Lt}} \varphi$. However, this is contradictory, since by definition of $\max_{\mathtt{size}}(.)$ for all $\beta' > \max_{\mathtt{size}}(\varphi)$, $\mathtt{size} \geqslant \beta' \not\subseteq_{\mathtt{Lt}} \varphi$. Thus, $\max_{\mathtt{size}}(\varphi) + \max_{\mathtt{size}}(\psi) = \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi))$. □

Proof of (**B**). Let $\beta \in \mathbb{N}$ such that $\neg\mathtt{size} \geqslant \beta \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi, \psi)$. By definition of $\langle * \rangle(\varphi, \psi)$, this implies that there are $\beta_1, \beta_2 \in [0, \alpha]$ such that $\beta = \beta_1 + \beta_2 \dot{-} 1$, $\neg\mathtt{size} \geqslant \beta_1 \subseteq_{\mathtt{Lt}} \varphi$ and $\neg\mathtt{size} \geqslant \beta_2 \subseteq_{\mathtt{Lt}} \psi$. Since φ and ψ are satisfiable, by definition of $\max_{\mathtt{size}}(.)$, we derive that $\beta_1 > \max_{\mathtt{size}}(\varphi)$ and $\beta_2 > \max_{\mathtt{size}}(\psi)$. This implies that the core formula $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1$ belongs to $\mathsf{Core}(\mathtt{X}, \alpha)$ and, analogously, that the core formula $\mathtt{size} \geqslant \max_{\mathtt{size}}(\psi) + 1$ belongs to $\mathsf{Core}(\mathtt{X}, \alpha)$. Since φ is in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, this implies that $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1$ is an atomic formula appearing in φ. By definition of $\max_{\mathtt{size}}(\varphi)$, the formula cannot appear positively, i.e. $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathtt{Lt}} \varphi$. Analogously, ψ is in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, which leads to $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\psi) + 1 \subseteq_{\mathtt{Lt}} \psi$. □

Proof of (**C**). Directly from (**A**) and (**B**). Indeed, by definition of $\langle * \rangle(\varphi, \psi)$, we know that for every $\neg\mathtt{size} \geqslant \beta \subseteq_{\mathtt{Lt}} \varphi$ and every $\neg\mathtt{size} \geqslant \beta' \subseteq_{\mathtt{Lt}} \psi$, $\neg\mathtt{size} \geqslant \beta + \beta' \dot{-} 1 \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi, \psi)$. □

Now, let us consider $\beta_g = \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi)) \dot{-} n$. We define the formula *Garb* below:

$$\mathit{Garb} \stackrel{\text{def}}{=} \begin{cases} \mathtt{size} = \beta_g & \text{if } \neg\mathtt{size} \geqslant \beta \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi, \psi), \text{ for some } \beta \\ \mathtt{size} \geqslant \beta_g & \text{otherwise,} \end{cases}$$

where we recall that $\mathtt{size} = \beta_g$ stands for $\mathtt{size} \geqslant \beta_g \wedge \neg(\mathtt{size} \geqslant \beta_g + 1)$. Notice that *Garb* is a conjunction of literals where at least one $\mathtt{size} \geqslant \beta$ occurs positively (i.e. $\mathtt{size} \geqslant 0$). The objective of this step of the proof is to show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \mathit{Alloc} * \mathit{Garb}$. First, we focus on the positive part of *Garb*, and prove $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \mathit{Alloc} * \mathtt{size} \geqslant \beta_g$. If $\beta_g = 0$ then $\mathtt{size} \geqslant \beta_g = \top$ and we have already shown $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \mathit{Alloc} * \top$. So, let us assume that $\beta_g > 1$. Notice that then $\max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi)) \dot{-} n = \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi)) - n$. We have

1	$\top \Rightarrow \mathtt{size} \geqslant \beta_g \vee \neg\mathtt{size} \geqslant \beta_g$	PC
2	$\mathit{Alloc} * \top \Rightarrow \mathit{Alloc} * (\mathtt{size} \geqslant \beta_g \vee \neg\mathtt{size} \geqslant \beta_g)$	$*$**-Intro**, $\mathbf{(A_7^*)}$, 1
3	$\mathit{Alloc} * (\mathtt{size} \geqslant \beta_g \vee \neg\mathtt{size} \geqslant \beta_g) \Rightarrow$ $(\mathit{Alloc} * \mathtt{size} \geqslant \beta_g) \vee (\mathit{Alloc} * \neg\mathtt{size} \geqslant \beta_g)$	$\mathbf{(I_9^*)}$, $\mathbf{(A_7^*)}$
4	$\mathit{Alloc} \Rightarrow \neg\mathtt{size} \geqslant n + 1$	Previously derived

5	$\mathit{Alloc} * \neg\mathtt{size} \geqslant \beta_g \Rightarrow (\neg\mathtt{size} \geqslant n+1) * \neg\mathtt{size} \geqslant \beta_g$	$*$**-Intro**, 4
6	$(\neg\mathtt{size} \geqslant n+1) * \neg\mathtt{size} \geqslant \beta_g \Rightarrow \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi))$	$\mathbf{(A^*_{19})}$, def. of β_g
7	$\mathit{Alloc} * \top \Rightarrow (\mathit{Alloc} * \mathtt{size} \geqslant \beta_g) \vee \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi))$	PC, 2, 3, 5, 6
8	$\langle * \rangle(\varphi,\psi) \Rightarrow \mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi))$	PC, def. of $\max_{\mathtt{size}}(.)$
9	$\langle * \rangle(\varphi,\psi) \Rightarrow \mathit{Alloc} * \top$	Previously derived
10	$\langle * \rangle(\varphi,\psi) \Rightarrow (\mathit{Alloc} * \mathtt{size} \geqslant \beta_g) \vee \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi))$	$\Rightarrow$**-Tr**, 7, 9
11	$\langle * \rangle(\varphi,\psi) \Rightarrow \mathit{Alloc} * \mathtt{size} \geqslant \beta_g$	PC, 8, 10

If for every β, $\neg\mathtt{size} \geqslant \beta \nsubseteq_{\mathtt{Lt}} \langle * \rangle(\varphi,\psi)$, then by definition of *Garb* we conclude that

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi,\psi) \Rightarrow \mathit{Alloc} * \mathit{Garb}.$$

Otherwise, suppose that there is β such that $\neg\mathtt{size} \geqslant \beta \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi,\psi)$. So, *Garb* is defined as $\mathtt{size} \geqslant \beta_g \wedge \neg(\mathtt{size} \geqslant \beta_g + 1)$. Directly from (**C**), we know that $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi)) + 1 \subseteq_{\mathtt{Lt}} \langle * \rangle(\varphi,\psi)$. By propositional reasoning,

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi,\psi) \Rightarrow \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi)) + 1.$$

Then, $\langle * \rangle(\varphi,\psi) \Rightarrow \mathit{Alloc} * \mathit{Garb}$ is derived as follows:

1	$\mathtt{size} \geqslant \beta_g \Rightarrow (\mathtt{size} \geqslant \beta_g \wedge \mathtt{size} \geqslant \beta_g + 1) \vee \mathtt{size} = \beta_g$	PC, def. of $\mathtt{size} = \beta_g$
2	$\mathit{Alloc} * \mathtt{size} \geqslant \beta_g \Rightarrow$ $\mathit{Alloc} * \big((\mathtt{size} \geqslant \beta_g \wedge \mathtt{size} \geqslant \beta_g + 1) \vee \mathtt{size} = \beta_g\big)$	$*$**-Intro**, $\mathbf{(A^*_7)}$, 1
3	$\mathit{Alloc} * \big((\mathtt{size} \geqslant \beta_g \wedge \mathtt{size} \geqslant \beta_g + 1) \vee \mathtt{size} = \beta_g\big)$ $\Rightarrow \big(\mathit{Alloc} * (\mathtt{size} \geqslant \beta_g \wedge \mathtt{size} \geqslant \beta_g + 1)\big) \vee \big(\mathit{Alloc} * \mathtt{size} = \beta_g\big)$	$\mathbf{(I^*_9)}$, $\mathbf{(A^*_7)}$
4	$\mathtt{size} \geqslant \beta_g \wedge \mathtt{size} \geqslant \beta_g + 1 \Rightarrow \mathtt{size} \geqslant \beta_g + 1$	PC
5	$\mathit{Alloc} \Rightarrow \mathtt{size} \geqslant n$	Previously derived
6	$\mathit{Alloc} * (\mathtt{size} \geqslant \beta_g \wedge \mathtt{size} \geqslant \beta_g + 1) \Rightarrow \mathtt{size} \geqslant n * \mathtt{size} \geqslant \beta_g + 1$	$*$**-Ilr**, 4, 5
7	$\mathtt{size} \geqslant n * \mathtt{size} \geqslant \beta_g + 1 \Rightarrow \mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi)) + 1$	$\mathbf{(A^*_8)}$, def. of $\mathtt{size} \geqslant \beta$
8	$\mathit{Alloc} * \mathtt{size} \geqslant \beta_g \Rightarrow \mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi)) + 1$ $\vee \big(\mathit{Alloc} * \mathtt{size} = \beta_g\big)$	PC, 2, 3, 6, 7
9	$\langle * \rangle(\varphi,\psi) \Rightarrow \mathit{Alloc} * \mathtt{size} \geqslant \beta_g$	Previously derived
10	$\langle * \rangle(\varphi,\psi) \Rightarrow \mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi)) + 1 \vee \big(\mathit{Alloc} * \mathtt{size} = \beta_g\big)$	$\Rightarrow$**-Tr**, 8, 9
11	$\langle * \rangle(\varphi,\psi) \Rightarrow \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi,\psi)) + 1$	PC, see above
12	$\langle * \rangle(\varphi,\psi) \Rightarrow \big(\mathit{Alloc} * \underbrace{\mathtt{size} = \beta_g}_{\mathit{Garb}}\big)$	PC, 10, 11

Step 2, distributing alloc and size literals. In this step, we aim at showing that

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc} * \mathit{Garb} \Rightarrow \varphi^{(1)} * \psi^{(1)}$$

where $\varphi^{(1)}$ and $\psi^{(1)}$ are two formulae defined as follows:

$$\varphi^{(1)} \stackrel{\text{def}}{=} \begin{cases} \mathtt{size} = \max_{\mathtt{size}}(\varphi) \wedge \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\} & \text{if } \max_{\mathtt{size}}(\varphi) < \alpha \\ \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \wedge \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\} & \text{otherwise} \end{cases}$$

$$\psi^{(1)} \stackrel{\text{def}}{=} \begin{cases} \mathtt{size} = \max_{\mathtt{size}}(\psi) \wedge \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \psi \mid i \in [1,n]\} & \text{if } \max_{\mathtt{size}}(\psi) < \alpha \\ \mathtt{size} \geqslant \max_{\mathtt{size}}(\psi) \wedge \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \psi \mid i \in [1,n]\} & \text{otherwise} \end{cases}$$

We use the notations $\varphi^{(1)}$ and $\psi^{(1)}$ since later in the proof, we shall consider sequences of formulae $\varphi^{(1)}, \ldots, \varphi^{(k)}$ and $\psi^{(1)}, \ldots, \psi^{(k)}$ with increasing amount of literals. That is why, using $\varphi^{(1)}$ and $\psi^{(1)}$ at this early stage is meaningful. Before tackling this derivation, a few more steps are required. First of all, notice that, if there is a formula $\mathtt{alloc}(\mathtt{x})$ occurring both in φ and ψ, then, by definition of $\langle * \rangle(\varphi, \psi)$, $\mathtt{x} \neq \mathtt{x}$ occurs in $\langle * \rangle(\varphi, \psi)$. This contradicts the fact that $\langle * \rangle(\varphi, \psi)$ is satisfiable. Therefore, we derive that the set of variables $\mathtt{x}_1, \ldots, \mathtt{x}_n$ can be split into two disjoint subsets, the ones "allocated" in φ, and the others in ψ. Let n_φ (resp. n_ψ) denote the number of equivalence classes of variables allocated in φ (resp. ψ). Clearly, $n = n_\varphi + n_\psi$. Moreover, since φ and ψ are satisfiable core types in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, where $\alpha \geqslant \mathrm{card}(\mathtt{X})$, we must have $n_\varphi \leqslant \max_{\mathtt{size}}(\varphi)$ and $n_\psi \leqslant \max_{\mathtt{size}}(\psi)$ (see the axiom $\mathbf{(I_6^C)}$). By $(\mathbf{A})$, we conclude that $n \leqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi))$. We define the following formulae

$$\mathit{Alloc}(\varphi) \stackrel{\text{def}}{=} \circledast\{\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \mid \mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi,\ i \in [1,n]\}$$

$$\mathit{Garb}(\varphi) \stackrel{\text{def}}{=} \begin{cases} \mathtt{size} = \max_{\mathtt{size}}(\varphi) - n_\varphi & \text{if } \max_{\mathtt{size}}(\varphi) < \alpha \\ \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) - n_\varphi & \text{otherwise} \end{cases}$$

Notice that, since $\max_{\mathtt{size}}(\varphi) \geqslant n_\varphi$, the formula $\mathit{Garb}(\varphi)$ is well-defined. The formulae $\mathit{Alloc}(\psi)$ and $\mathit{Garb}(\psi)$ are defined accordingly. Obviously, Alloc is equal to $\mathit{Alloc}(\varphi) * \mathit{Alloc}(\psi)$ modulo associativity and commutativity of the separating conjunction $*$. Hence, by taking advantage of the axioms $\mathbf{(A_7^*)}$ and $\mathbf{(A_8^*)}$, we have

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc} \Leftrightarrow \mathit{Alloc}(\varphi) * \mathit{Alloc}(\psi).$$

Let us now look at $\mathit{Garb}(\varphi)$ and $\mathit{Garb}(\psi)$. We aim at deriving

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Garb} \Rightarrow \mathit{Garb}(\varphi) * \mathit{Garb}(\psi).$$

Since φ is a core type, we know that if $\max_{\mathtt{size}}(\varphi) < \alpha$ then, by definition of $\max_{\mathtt{size}}(\varphi)$, $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathtt{Lt}} \varphi$. A similar analysis can be done for ψ, which leads to the two following equivalences, by definition of $\mathit{Garb}(\varphi)$ and $\mathit{Garb}(\psi)$:

- $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathtt{Lt}} \varphi$ if and only if $\mathit{Garb}(\varphi) = (\mathtt{size} = \max_{\mathtt{size}}(\varphi) - n_\varphi)$,
- $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\psi) + 1 \subseteq_{\mathtt{Lt}} \psi$ if and only if $\mathit{Garb}(\psi) = (\mathtt{size} = \max_{\mathtt{size}}(\psi) - n_\psi)$.

By definition of Garb, $(\mathbf{B})$ and $(\mathbf{C})$, we know that $\mathit{Garb} = (\mathtt{size} = \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi)) \dot{-} n)$ holds if and only if $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathtt{Lt}} \varphi$ and $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathtt{Lt}} \psi$. From $n \leqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi))$ and by relying on the previous two equivalences, this allows us to conclude that:

D. $\mathit{Garb}(\varphi) = (\mathtt{size} = \max_{\mathtt{size}}(\varphi) - n_\varphi)$ and $\mathit{Garb}(\psi) = (\mathtt{size} = \max_{\mathtt{size}}(\psi) - n_\psi)$ if and only if $\mathit{Garb} = (\mathtt{size} = \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi)) - n)$.

To show $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Garb} \Rightarrow (\mathit{Garb}(\varphi) * \mathit{Garb}(\psi))$, we split the proof depending on whether $\mathit{Garb}(\varphi) = (\mathtt{size} = \max_{\mathtt{size}}(\varphi) - n_\varphi)$ and $\mathit{Garb}(\psi) = (\mathtt{size} = \max_{\mathtt{size}}(\psi) - n_\psi)$ hold.

case: $\mathit{Garb}(\varphi) \neq (\mathtt{size} = \max_{\mathtt{size}}(\varphi){-}n_\varphi)$ **and** $\mathit{Garb}(\psi) \neq (\mathtt{size} = \max_{\mathtt{size}}(\psi){-}n_\psi)$**:** We have $\mathit{Garb}(\varphi) = (\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi){-}n_\varphi)$ and $\mathit{Garb}(\psi) = (\mathtt{size} \geqslant \max_{\mathtt{size}}(\psi){-}n_\psi)$. By definition of *Garb* and (**D**), $\mathit{Garb} = (\mathtt{size} \geqslant \max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi)) - n)$. By $n = n_\varphi + n_\psi$ and (**A**), $\max_{\mathtt{size}}(\langle * \rangle(\varphi, \psi)) - n = (\max_{\mathtt{size}}(\varphi){-}n_\varphi) + (\max_{\mathtt{size}}(\psi){-}n_\psi)$. By definition of the core formula $\mathtt{size} \geqslant \beta$, *Garb* is already equivalent to $\mathit{Garb}(\varphi) * \mathit{Garb}(\psi)$, modulo associativity and commutativity of the separating conjunction $*$. Hence, by taking advantage of the axioms $\mathbf{(A_7^*)}$ and $\mathbf{(A_8^*)}$, we have $\vdash_{\mathcal{H}_\mathsf{C}(*)} \mathit{Garb} \Rightarrow \mathit{Garb}(\varphi) * \mathit{Garb}(\psi)$.

case: $\mathit{Garb}(\varphi) = (\mathtt{size} = \max_{\mathtt{size}}(\varphi){-}n_\varphi)$ **and** $\mathit{Garb}(\psi) \neq (\mathtt{size} = \max_{\mathtt{size}}(\psi){-}n_\psi)$**:** We have $\mathit{Garb}(\psi) = (\mathtt{size} \geqslant \max_{\mathtt{size}}(\psi){-}n_\psi)$ and, by definition of *Garb* and (**D**), together with $n = n_\varphi + n_\psi$ and (**A**), $\mathit{Garb} = (\mathtt{size} \geqslant (\max_{\mathtt{size}}(\varphi){-}n_\varphi) + (\max_{\mathtt{size}}(\psi){-}n_\psi))$. In this case, $\mathit{Garb} \Rightarrow \mathit{Garb}(\varphi) * \mathit{Garb}(\psi)$ is an instantiation of the following valid formula with $\beta_1 = \max_{\mathtt{size}}(\varphi){-}n_\varphi$ and $\beta_2 = \max_{\mathtt{size}}(\psi) - n_\psi$:

$$\mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} \geqslant \beta_2.$$

The derivability of this formula in $\mathcal{H}_\mathsf{C}(*)$ is proven by induction on β_1 (see Appendix B).

case: $\mathit{Garb}(\varphi) \neq (\mathtt{size} = \max_{\mathtt{size}}(\varphi){-}n_\varphi)$ **and** $\mathit{Garb}(\psi) = (\mathtt{size} = \max_{\mathtt{size}}(\psi){-}n_\psi)$**:** Analogously to the previous case, we have $\mathit{Garb}(\varphi) = (\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi){-}n_\varphi)$ and $\mathit{Garb} = (\mathtt{size} \geqslant (\max_{\mathtt{size}}(\varphi){-}n_\varphi) + (\max_{\mathtt{size}}(\psi){-}n_\psi))$. We instantiate the theorem

$$\mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} \geqslant \beta_2,$$

shown derivable in the previous case of the proof, with $\beta_1 = \max_{\mathtt{size}}(\psi){-}n_\psi$ and $\beta_2 = \max_{\mathtt{size}}(\varphi) - n_\varphi$. This corresponds to $\mathit{Garb} \Rightarrow \mathit{Garb}(\psi) * \mathit{Garb}(\varphi)$. Afterwards, by commutativity of the separating conjunction (axiom $\mathbf{(A_7^*)}$) and propositional reasoning, we conclude that $\vdash_{\mathcal{H}_\mathsf{C}(*)} \mathit{Garb} \Rightarrow \mathit{Garb}(\varphi) * \mathit{Garb}(\psi)$.

case: $\mathit{Garb}(\varphi) = (\mathtt{size} = \max_{\mathtt{size}}(\varphi){-}n_\varphi)$ **and** $\mathit{Garb}(\psi) = (\mathtt{size} = \max_{\mathtt{size}}(\psi){-}n_\psi)$**:** By (**D**), $n = n_\varphi + n_\psi$ and (**A**), $\mathit{Garb} = (\mathtt{size} = (\max_{\mathtt{size}}(\varphi){-}n_\varphi) + (\max_{\mathtt{size}}(\psi){-}n_\psi))$. In this case, $\mathit{Garb} \Rightarrow \mathit{Garb}(\varphi) * \mathit{Garb}(\psi)$ is an instantiation of the following valid formula, with $\beta_1 = \max_{\mathtt{size}}(\varphi){-}n_\varphi$ and $\beta_2 = \max_{\mathtt{size}}(\psi) - n_\psi$:

$$\mathtt{size} = \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} = \beta_2.$$

Its derivation in $\mathcal{H}_\mathsf{C}(*)$ can be found in Appendix B.

Thanks to the case analysis above, we conclude that $\vdash_{\mathcal{H}_\mathsf{C}(*)} \mathit{Garb} \Rightarrow \mathit{Garb}(\varphi) * \mathit{Garb}(\psi)$. Thus, $\vdash_{\mathcal{H}_\mathsf{C}(*)} \mathit{Alloc} * \mathit{Garb} \Rightarrow (\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi)) * (\mathit{Alloc}(\psi) * \mathit{Garb}(\psi))$. Indeed,

1	$\mathit{Alloc} \Rightarrow \mathit{Alloc}(\varphi) * \mathit{Alloc}(\psi)$	Previously derived
2	$\mathit{Garb} \Rightarrow \mathit{Garb}(\varphi) * \mathit{Garb}(\psi)$	Previously derived
3	$\mathit{Alloc} * \mathit{Garb} \Rightarrow (\mathit{Alloc}(\varphi) * \mathit{Alloc}(\psi)) * (\mathit{Garb}(\varphi) * \mathit{Garb}(\psi))$	$*$**-Ilr**, 1, 2
4	$(\mathit{Alloc}(\varphi) * \mathit{Alloc}(\psi)) * (\mathit{Garb}(\varphi) * \mathit{Garb}(\psi)) \Rightarrow$ $(\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi)) * (\mathit{Alloc}(\psi) * \mathit{Garb}(\psi))$	$\mathbf{(A_7^*)}$, $\mathbf{(A_8^*)}$
5	$\mathit{Alloc} * \mathit{Garb} \Rightarrow (\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi)) * (\mathit{Alloc}(\psi) * \mathit{Garb}(\psi))$	$\Rightarrow$**-Tr**, 3, 4

To conclude this step of the proof, it is sufficient to show $\vdash_{\mathcal{H}_\mathsf{C}(*)} \mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \varphi^{(1)}$ and $\vdash_{\mathcal{H}_\mathsf{C}(*)} \mathit{Alloc}(\psi) * \mathit{Garb}(\psi) \Rightarrow \psi^{(1)}$. Indeed, by relying on the rule $*$**-Ilr**, we then obtain $\vdash_{\mathcal{H}_\mathsf{C}(*)} \mathit{Alloc} * \mathit{Garb} \Rightarrow \varphi^{(1)} * \psi^{(1)}$. Below, we show $\vdash_{\mathcal{H}_\mathsf{C}(*)} \mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \varphi^{(1)}$. The developments of $\vdash_{\mathcal{H}_\mathsf{C}(*)} \mathit{Alloc}(\psi) * \mathit{Garb}(\psi) \Rightarrow \psi^{(1)}$ are analogous. We recall that the formula

$\mathit{Alloc}(\varphi)$ is defined as

$$\mathit{Alloc}(\varphi) \;=\; \circledast\{\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \mid \mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi\}.$$

First of all, let us show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc}(\varphi) * \top \Rightarrow \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\}$. The proof is divided in three cases:

case: $\{\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \mid \mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi\} = \varnothing$**:** In this case, the formula we want to derive is syntactically equal to $\top * \top \Rightarrow \top$, which is derivable by propositional reasoning.

case: $\mathrm{card}(\{\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \mid \mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi\}) = 1$**:** In this case, the formula we want to derive is syntactically equal to $(\mathtt{alloc}(\mathtt{x}) \wedge \mathtt{size} = 1) * \top \Rightarrow \mathtt{alloc}(\mathtt{x})$. Therefore, it is derivable in $\mathcal{H}_{\mathsf{C}}(*)$ by $\mathbf{(I^*_{12})}$ and $*$**-Intro**.

case: $\mathrm{card}(\{\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \mid \mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi\}) \geqslant 2$**:** In the derivation below, we write $\mathit{Alloc}(\varphi)^{-i}$ for $\circledast\{\mathtt{alloc}(\mathtt{x}_j) \wedge \mathtt{size} = 1 \mid j \in [1,n]\backslash\{i\}, \mathtt{alloc}(\mathtt{x}_j) \subseteq_{\mathtt{Lt}} \varphi\}$. Roughly speaking, $\mathit{Alloc}(\varphi)^{-i}$ is obtained from $\mathit{Alloc}(\varphi)$ by removing the subformula $\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1$. Since $\mathrm{card}(\{\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \mid \mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi\}) \geqslant 2$, the formula $\mathit{Alloc}(\varphi)^{-i}$ is different from $\top$. We have

1	$\mathit{Alloc}(\varphi) * \top \Rightarrow$ $(\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1) * (\mathit{Alloc}(\varphi)^{-i} * \top)$	$\mathbf{(A^*_7)}$, $\mathbf{(A^*_8)}$, def. of $\mathit{Alloc}(\varphi)$ where $\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi$ and $i \in [1,n]$
2	$\mathit{Alloc}(\varphi)^{-i} * \top \Rightarrow \top$	PC
3	$\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \Rightarrow \mathtt{alloc}(\mathtt{x}_i)$	PC
4	$(\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1) * (\mathit{Alloc}(\varphi)^{-i} * \top) \Rightarrow$ $\mathtt{alloc}(\mathtt{x}_i) * \top$	$*$**-Ilr**, 2, 3
5	$\mathtt{alloc}(\mathtt{x}_i) * \top \Rightarrow \mathtt{alloc}(\mathtt{x}_i)$	$\mathbf{(I^*_{12})}$
6	$\mathit{Alloc}(\varphi) * \top \Rightarrow \mathtt{alloc}(\mathtt{x}_i)$	$\Rightarrow$**-Tr**, 1, 4, 5
7	$\mathit{Alloc}(\varphi) * \top \Rightarrow \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\}$	PC, repeating 6 for all $i \in [1,n]$ such that $\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi$

So, we have $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc}(\varphi) * \top \Rightarrow \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\}$.
Now, recall that $\mathrm{card}(\{i \in [1,n] \mid \mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi\}) = n_\varphi$. At the beginning of the proof, we have shown a derivation of $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc} \Rightarrow \mathtt{size} = n$, where Alloc is defined as $\circledast\{\mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \mid i \in [1,n]\}$. Replacing Alloc by $\mathit{Alloc}(\varphi)$ and n by n_φ in the derivation of $\mathit{Alloc} \Rightarrow \mathtt{size} = n$ leads to a derivation in $\mathcal{H}_{\mathsf{C}}(*)$ of $\mathit{Alloc}(\varphi) \Rightarrow \mathtt{size} = n_\varphi$.

To show $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \varphi^{(1)}$, we split the proof in two cases:

case: $\max_{\mathtt{size}}(\varphi) = \alpha$**:** By definition of $\varphi^{(1)}$ and $\mathit{Garb}(\varphi)$, we have:

- $\varphi^{(1)} \;=\; \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \wedge \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\}$,
- $\mathit{Garb}(\varphi) \;=\; \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) - n_\varphi$,

Then,

1	$\mathit{Alloc}(\varphi) * \top \Rightarrow \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\}$	Previously derived
2	$\mathit{Garb}(\varphi) \Rightarrow \top$	PC
3	$\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \mathit{Alloc}(\varphi) * \top$	$*$**-Intro**, $\mathbf{(A^*_7)}$, 2

4	$\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\}$	$\Rightarrow$**-Tr**, 1, 3
5	$\mathit{Alloc}(\varphi) \Rightarrow \mathtt{size} = n_\varphi$	See above
6	$\mathtt{size} = n_\varphi \Rightarrow \mathtt{size} \geqslant n_\varphi$	PC, def. of $\mathtt{size} = n_\varphi$
7	$\mathit{Alloc}(\varphi) \Rightarrow \mathtt{size} \geqslant n_\varphi$	
8	$\mathit{Garb}(\varphi) \Rightarrow \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) - n_\varphi$	PC, def. of $\mathit{Garb}(\varphi)$
9	$\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \mathtt{size} \geqslant n_\varphi * \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) - n_\varphi$	$*$**-Ilr**, 7, 8
10	$\mathtt{size} \geqslant n_\varphi * \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) - n_\varphi \Rightarrow \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi)$	$\mathbf{(A_8^*)}$, $\mathbf{(A_7^*)}$, def. of $\mathtt{size} \geqslant \beta$
11	$\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi)$	$\Rightarrow$**-Tr**, 9, 10
12	$\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \varphi^{(1)}$	PC, 4, 11, def. of $\varphi^{(1)}$

case: $\max_{\mathtt{size}}(\varphi) \neq \alpha$**:** In this case, $\max_{\mathtt{size}}(\varphi) < \alpha$ and so we have:

- $\varphi^{(1)} = \mathtt{size} = \max_{\mathtt{size}}(\varphi) \wedge \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\}$,
- $\mathit{Garb}(\varphi) = \mathtt{size} = \max_{\mathtt{size}}(\varphi) - n_\varphi$,

We can rely on the previous case of the proof in order to show that

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \wedge \bigwedge\{\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi \mid i \in [1,n]\}.$$

By propositional reasoning, we can derive $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \varphi^{(1)}$ as soon as we show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1$, as we do now:

1	$\mathit{Alloc}(\varphi) \Rightarrow \mathtt{size} = n_\varphi$	Already discussed above
2	$\mathtt{size} = n_\varphi \Rightarrow \neg\mathtt{size} \geqslant n_\varphi + 1$	PC, def. of $\mathtt{size} = n_\varphi$
3	$\mathit{Alloc}(\varphi) \Rightarrow \neg\mathtt{size} \geqslant n_\varphi + 1$	PC, $\Rightarrow$**-Tr**, 1, 2
4	$\mathit{Garb}(\varphi) \Rightarrow \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) - n_\varphi + 1$	PC, def. of $\mathtt{size} = \beta$
5	$\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow$ $\neg\mathtt{size} \geqslant n_\varphi + 1 * \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) - n_\varphi + 1$	$*$**-Ilr**, 3, 4
6	$\neg\mathtt{size} \geqslant n_\varphi + 1 * \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) - n_\varphi + 1 \Rightarrow$ $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1$	$\mathbf{(A_{19}^*)}$
7	$\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1$	$\Rightarrow$**-Tr**, 5, 6

This concludes the proof of $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi) \Rightarrow \varphi^{(1)}$. As already stated, one can analogously show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc}(\psi) * \mathit{Garb}(\psi) \Rightarrow \psi^{(1)}$. Afterwards, by $*$**-Ilr** and from $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc} * \mathit{Garb} \Rightarrow (\mathit{Alloc}(\varphi) * \mathit{Garb}(\varphi)) * (\mathit{Alloc}(\psi) * \mathit{Garb}(\psi))$, we conclude that

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \mathit{Alloc} * \mathit{Garb} \Rightarrow \varphi^{(1)} * \psi^{(1)}.$$

Step 3, add the missing literals. From the first and second step of the proof, and by propositional reasoning, $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(1)} * \psi^{(1)}$. We now rely on $\langle * \rangle(\varphi, \psi)$ to add to $\varphi^{(1)}$ and $\psi^{(1)}$ missing literals from φ and ψ, respectively. We add the literals progressively, building a sequence of formulae $\varphi^{(1)} * \psi^{(1)}$, $\varphi^{(2)} * \psi^{(2)}$, …, $\varphi^{(k)} * \psi^{(k)}$, where for all $i \in [1,k]$, $\varphi^{(i)}$ and $\psi^{(i)}$ are conjunctions of core formulae such that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$, and

for all $j \in [1, i]$, $\varphi^{(j)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$ and $\psi^{(j)} \subseteq_{\mathsf{Lt}} \psi^{(i)}$. Fundamentally, we obtain $\varphi = \varphi^{(k)}$ and $\psi = \psi^{(k)}$ (modulo associativity and commutativity of the classical conjunction), which allows us to derive $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi * \psi$, ending the proof. Below, we focus on the formula $\varphi^{(i)}$ and φ. Since $\langle * \rangle(\varphi, \psi)$ is equal to $\langle * \rangle(\psi, \varphi)$ (by definition) and the separating conjunction is commutative (axiom $\mathbf{(A_7^*)}$), a similar analysis can be done for $\psi^{(i)}$ and ψ. Thus, we assume that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$ holds, where in particular $\varphi^{(1)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$ and $\psi^{(1)} \subseteq_{\mathsf{Lt}} \psi^{(i)}$, and that there is a literal $L \subseteq_{\mathsf{Lt}} \varphi$ that does not appear in $\varphi^{(i)}$. By relying on the theorems in Lemma 5.2, we show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \langle * \rangle(\varphi, \psi) \Rightarrow (\varphi^{(i)} \wedge L) * \psi^{(i)}$ by a case analysis on L.

case: $L = \mathtt{x} \sim \mathtt{y}$**, where** $\sim \in \{=, \neq\}$**:** By definition of $\langle * \rangle(\varphi, \psi)$, $\mathtt{x} \sim \mathtt{y} \subseteq_{\mathsf{Lt}} \langle * \rangle(\varphi, \psi)$.

1	$\langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$	Hypothesis
2	$\langle * \rangle(\varphi, \psi) \Rightarrow \mathtt{x} \sim \mathtt{y}$	PC, def. of $\langle * \rangle(\varphi, \psi)$, see above
3	$\langle * \rangle(\varphi, \psi) \Rightarrow \mathtt{x} \sim \mathtt{y} \wedge (\varphi^{(i)} * \psi^{(i)})$	PC, 1, 2
4	$\mathtt{x} \sim \mathtt{y} \wedge (\varphi^{(i)} * \psi^{(i)}) \Rightarrow (\varphi^{(i)} \wedge \mathtt{x} \sim \mathtt{y}) * \psi^{(i)}$	$\mathbf{(I^*_{5.2.1})}$
5	$\langle * \rangle(\varphi, \psi) \Rightarrow (\varphi^{(i)} \wedge \mathtt{x} \sim \mathtt{y}) * \psi^{(i)}$	$\Rightarrow$**-Tr**, 3, 4

case: $L = \mathtt{alloc(x)}$**:** Since $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$, by definition, $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \langle * \rangle(\varphi, \psi)$. By definition of $\mathtt{x}_1, \ldots, \mathtt{x}_n$, there is $j \in [1, n]$ such that $\mathtt{x}_j = \mathtt{x} \subseteq_{\mathsf{Lt}} \langle * \rangle(\varphi, \psi)$. Since φ is a core type, $\mathtt{alloc}(\mathtt{x}_j) \subseteq_{\mathsf{Lt}} \varphi$. By definition of $\varphi^{(1)}$, $\mathtt{alloc}(\mathtt{x}_j) \subseteq_{\mathsf{Lt}} \varphi^{(1)}$. From $\varphi^{(1)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$, we have $\mathtt{alloc}(\mathtt{x}_j) \subseteq_{\mathsf{Lt}} \varphi^{(i)}$. Afterwards,

1	$\varphi^{(i)} \Rightarrow \varphi^{(i)} \wedge \mathtt{alloc}(\mathtt{x}_j)$	PC, see above
2	$\langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$	Hypothesis
3	$\varphi^{(i)} * \psi^{(i)} \Rightarrow (\varphi^{(i)} \wedge \mathtt{alloc}(\mathtt{x}_j)) * \psi^{(i)}$	$*$**-Intro**, 1
4	$\langle * \rangle(\varphi, \psi) \Rightarrow \mathtt{x}_j = \mathtt{x}$	PC, see above
5	$\langle * \rangle(\varphi, \psi) \Rightarrow \mathtt{x}_j = \mathtt{x} \wedge ((\varphi^{(i)} \wedge \mathtt{alloc}(\mathtt{x}_j)) * \psi^{(i)})$	PC, 2, 3, 4
6	$\mathtt{x}_j = \mathtt{x} \wedge ((\varphi^{(i)} \wedge \mathtt{alloc}(\mathtt{x}_j)) * \psi^{(i)}) \Rightarrow (\varphi^{(i)} \wedge \mathtt{alloc}(\mathtt{x})) * \psi^{(i)}$	$\mathbf{(I^*_{5.2.2})}$
7	$\langle * \rangle(\varphi, \psi) \Rightarrow ((\varphi^{(i)} \wedge \mathtt{alloc}(\mathtt{x})) * \psi^{(i)})$	$\Rightarrow$**-Tr**, 5, 6

Without loss of generality, thanks to the derivation above dealing with $\mathtt{alloc(x)}$ literals, we now assume that for all $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$ and all $\mathtt{alloc(y)} \subseteq_{\mathsf{Lt}} \psi$, we have $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$ and $\mathtt{alloc(y)} \subseteq_{\mathsf{Lt}} \psi^{(i)}$.

case: $L = \neg\mathtt{alloc(x)}$**:** We distinguish two main subcases.

- First, assume $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \psi$. By definition of $\langle * \rangle(\varphi, \psi)$, $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \langle * \rangle(\varphi, \psi)$.

1	$\langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$	Hypothesis
2	$\langle * \rangle(\varphi, \psi) \Rightarrow \neg\mathtt{alloc}(\mathtt{x})$	PC, def. of $\langle * \rangle(\varphi, \psi)$, see above
3	$\langle * \rangle(\varphi, \psi) \Rightarrow \neg\mathtt{alloc}(\mathtt{x}) \wedge (\varphi^{(i)} * \psi^{(i)})$	PC, 1, 2
4	$\neg\mathtt{alloc}(\mathtt{x}) \wedge (\varphi^{(i)} * \psi^{(i)}) \Rightarrow (\varphi^{(i)} \wedge \neg\mathtt{alloc}(\mathtt{x})) * \psi^{(i)}$	$\mathbf{(I^*_{5.2.4})}$
5	$\langle * \rangle(\varphi, \psi) \Rightarrow (\varphi^{(i)} \wedge \neg\mathtt{alloc}(\mathtt{x})) * \psi^{(i)}$	$\Rightarrow$**-Tr**, 3, 4

- Otherwise, $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \psi$. By assumption, $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \psi^{(i)}$.

1	$\psi^{(i)} \Rightarrow \psi^{(i)} \wedge \mathtt{alloc(x)}$	PC, see above
2	$\langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$	Hypothesis
3	$\varphi^{(i)} * \psi^{(i)} \Rightarrow (\psi^{(i)} \wedge \mathtt{alloc(x)}) * \varphi^{(i)}$	$\mathbf{(A_7^*)}$, $*$**-Intro**, 1
4	$(\psi^{(i)} \wedge \mathtt{alloc(x)}) * \varphi^{(i)} \Rightarrow \psi^{(i)} * (\varphi^{(i)} \wedge \neg\mathtt{alloc(x)})$	$\mathbf{(I^*_{5.2.3})}$
5	$\psi^{(i)} * (\varphi^{(i)} \wedge \neg\mathtt{alloc(x)}) \Rightarrow (\varphi^{(i)} \wedge \neg\mathtt{alloc(x)}) * \psi^{(i)}$	$\mathbf{(A_7^*)}$
6	$\langle * \rangle(\varphi, \psi) \Rightarrow (\varphi^{(i)} \wedge \neg\mathtt{alloc(x)}) * \psi^{(i)}$	$\Rightarrow$**-Tr**, 2, 3, 4, 5

case: $L = \mathtt{x} \hookrightarrow \mathtt{y}$**:** Similar to the case $L = \mathtt{alloc(x)}$. Since φ is a satisfiable core type, we have $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$ (see axiom $\mathbf{(A_3^C)}$). By assumption, $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$. By definition of $\langle * \rangle(\varphi, \psi)$, we have $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \langle * \rangle(\varphi, \psi)$.

1	$\varphi^{(i)} \Rightarrow \varphi^{(i)} \wedge \mathtt{alloc(x)}$	PC, see above
2	$\langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$	Hypothesis
3	$\langle * \rangle(\varphi, \psi) \Rightarrow \mathtt{x} \hookrightarrow \mathtt{y}$	PC, see above
4	$\varphi^{(i)} * \psi^{(i)} \Rightarrow (\varphi^{(i)} \wedge \mathtt{alloc(x)}) * \psi^{(i)}$	$*$**-Intro**, 1
5	$\langle * \rangle(\varphi, \psi) \Rightarrow \mathtt{x} \hookrightarrow \mathtt{y} \wedge ((\varphi^{(i)} \wedge \mathtt{alloc(x)}) * \psi^{(i)})$	PC, 3, 4
6	$\mathtt{x} \hookrightarrow \mathtt{y} \wedge ((\varphi^{(i)} \wedge \mathtt{alloc(x)}) * \psi^{(i)}) \Rightarrow (\varphi^{(i)} \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi^{(i)}$	$\mathbf{(I^*_{5.2.6})}$
7	$\langle * \rangle(\varphi, \psi) \Rightarrow (\varphi^{(i)} \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi^{(i)}$	$*$**-Intro**, 5, 6

Without loss of generality, thanks to the previous cases dealing with $\neg\mathtt{alloc(x)}$ literals, below we assume that for every $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$ and every $\neg\mathtt{alloc(y)} \subseteq_{\mathsf{Lt}} \psi$, we have $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$ and $\neg\mathtt{alloc(y)} \subseteq_{\mathsf{Lt}} \psi^{(i)}$.

case: $L = \neg\mathtt{x} \hookrightarrow \mathtt{y}$**:** We distinguish two main subcases

- First, suppose $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$. In this case, by definition of $\langle * \rangle(\varphi, \psi)$, we have $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \langle * \rangle(\varphi, \psi)$. Therefore,

1	$\langle * \rangle(\varphi, \psi) \Rightarrow \neg\mathtt{x} \hookrightarrow \mathtt{y}$	PC, see above
2	$\langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$	Hypothesis
3	$\langle * \rangle(\varphi, \psi) \Rightarrow \neg\mathtt{x} \hookrightarrow \mathtt{y} \wedge (\varphi^{(i)} * \psi^{(i)})$	PC, 1, 2
4	$\neg\mathtt{x} \hookrightarrow \mathtt{y} \wedge (\varphi^{(i)} * \psi^{(i)}) \Rightarrow (\varphi^{(i)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}) * \psi^{(i)}$	$\mathbf{(I^*_{5.2.7})}$

- Otherwise, we have $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$. By assumption, $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$, and thus

1	$\varphi^{(i)} \Rightarrow \neg\mathtt{alloc(x)}$	PC, see above
2	$\neg\mathtt{alloc(x)} \Rightarrow \neg\mathtt{x} \hookrightarrow \mathtt{y}$	$\mathbf{(A_3^C)}$, PC
3	$\varphi^{(i)} \Rightarrow \neg\mathtt{x} \hookrightarrow \mathtt{y}$	$\Rightarrow$**-Tr**, 1, 2
4	$\varphi^{(i)} \Rightarrow \varphi^{(i)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}$	PC, 3
5	$\langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$	Hypothesis

6	$\varphi^{(i)} * \psi^{(i)} \Rightarrow (\varphi^{(i)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y}) * \psi^{(i)}$	$*$**-Intro**, 4
7	$\langle * \rangle(\varphi, \psi) \Rightarrow (\varphi^{(i)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y}) * \psi^{(i)}$	$\Rightarrow$**-Tr**, 5, 6

case: $L = \mathtt{size} \geqslant \beta$**:** By definition of $\max_{\mathtt{size}}(.)$, $\beta \leqslant \max_{\mathtt{size}}(\varphi)$. By definition of $\varphi^{(1)}$, $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \subseteq_{\mathsf{Lt}} \varphi^{(1)}$. From $\varphi^{(1)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$, we get $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \subseteq_{\mathsf{Lt}} \varphi^{(i)}$.

1	$\varphi^{(i)} \Rightarrow \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi)$	PC, see above
2	$\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \Rightarrow \mathtt{size} \geqslant \beta$	repeated $\mathbf{(I_5^C)}$, PC, as $\beta \leqslant \max_{\mathtt{size}}(\varphi)$
3	$\varphi^{(i)} \Rightarrow \varphi^{(i)} \wedge \mathtt{size} \geqslant \beta$	PC, 1, 2
4	$\langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$	Hypothesis
5	$\varphi^{(i)} * \psi^{(i)} \Rightarrow (\varphi^{(i)} \wedge \mathtt{size} \geqslant \beta) * \psi^{(i)}$	$*$**-Intro**, 3
6	$\langle * \rangle(\varphi, \psi) \Rightarrow (\varphi^{(i)} \wedge \mathtt{size} \geqslant \beta) * \psi^{(i)}$	$\Rightarrow$**-Tr**, 4, 5

case: $L = \neg\mathtt{size} \geqslant \beta$**:** In this case, $\max_{\mathtt{size}}(\varphi) < \alpha$. Since φ is a satisfiable core type, we have $\beta > \max_{\mathtt{size}}(\varphi)$. Moreover, by definition of $\varphi^{(1)}$, $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathsf{Lt}} \varphi^{(1)}$. From $\varphi^{(1)} \subseteq_{\mathsf{Lt}} \varphi^{(i)}$, we have $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathsf{Lt}} \varphi^{(i)}$.

1	$\varphi^{(i)} \Rightarrow \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi)+1$	PC, see above
2	$\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi)+1 \Rightarrow \neg\mathtt{size} \geqslant \beta$	repeated $\mathbf{(I_5^C)}$, PC, as $\beta > \max_{\mathtt{size}}(\varphi)$ by PC, the contrapositive of $\mathbf{(I_5^C)}$ is derivable
3	$\varphi^{(i)} \Rightarrow \varphi^{(i)} \wedge \neg\mathtt{size} \geqslant \beta$	PC, 1, 2
4	$\langle * \rangle(\varphi, \psi) \Rightarrow \varphi^{(i)} * \psi^{(i)}$	Hypothesis
5	$\varphi^{(i)} * \psi^{(i)} \Rightarrow (\varphi^{(i)} \wedge \neg\mathtt{size} \geqslant \beta) * \psi^{(i)}$	$*$**-Intro**, 3
6	$\langle * \rangle(\varphi, \psi) \Rightarrow (\varphi^{(i)} \wedge \neg\mathtt{size} \geqslant \beta) * \psi^{(i)}$	$\Rightarrow$**-Tr**, 4, 5

□

Corollary 5.5 (Star elimination)**.** *Let* $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$ *and* $\alpha \geqslant \mathrm{card}(\mathtt{X})$*. Let* φ *and* ψ *in* $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$*. There is* χ *in* $\mathsf{Conj}(\mathsf{Core}(\mathtt{X}, 2\alpha))$ *such that* $\vdash_{\mathcal{H}_\mathsf{C}(*)} \varphi * \psi \Leftrightarrow \chi$*.*

Proof. If both φ and ψ are satisfiable, the results holds directly by Lemma 5.4, as $\langle * \rangle(\varphi, \psi)$ is in $\mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \alpha + \alpha))$. Otherwise, let us treat the case where one of the two formulas is unsatisfiable. For instance, assume that φ is unsatisfiable. Then $\vdash_{\mathcal{H}_\mathsf{C}} \varphi \Rightarrow \bot$ by completeness of $\mathcal{H}_\mathsf{C}$ (Lemma 4.1) and, $\mathcal{H}_\mathsf{C}(*)$ includes $\mathcal{H}_\mathsf{C}$, $\vdash_{\mathcal{H}_\mathsf{C}(*)} \varphi \Rightarrow \bot$. By the rule $*$**-Intro** and by the axiom $\mathbf{(I_{10}^*)}$, we get $\vdash_{\mathcal{H}_\mathsf{C}(*)} \varphi * \psi \Rightarrow \bot$. Thus χ can take the value $\neg(\mathtt{x} = \mathtt{x})$. The case where ψ is not satisfiable is analogous, thanks to $\mathbf{(A_7^*)}$. □

By the distributivity axiom $\mathbf{(I_9^*)}$, Corollary 5.5 is extended from core types to arbitrary Boolean combinations of core formulae. $\mathcal{H}_\mathsf{C}(*)$ is therefore complete for $\mathsf{SL}(*, \mathtt{alloc})$. In order to derive a valid formula $\varphi \in \mathsf{SL}(*, \mathtt{alloc})$, we repeatedly apply the elimination of $*$ in a bottom-up fashion, starting from the leaves of φ (which are Boolean combinations of core formulae) and obtaining a Boolean combination of core formulae ψ that is equivalent to φ. Then, we rely on the completeness of $\mathcal{H}_\mathsf{C}$ (Theorem 4.3) to prove that ψ is derivable.

Theorem 5.6. *A formula* φ *in* $\mathsf{SL}(*, \mathtt{alloc})$ *is valid iff* $\vdash_{\mathcal{H}_\mathsf{C}(*)} \varphi$*.*

Proof. Soundness of the proof system $\mathcal{H}_{\mathsf{C}}(*)$ has been already established earlier.

As far as the completeness proof is concerned, we need to show that for every formula φ in $\mathsf{SL}(*, \mathtt{alloc})$, there is a Boolean combination of core formulae ψ such that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi \Leftrightarrow \psi$. In order to conclude the proof, when φ is valid for $\mathsf{SL}(*, \mathtt{alloc})$, by soundness of $\mathcal{H}_{\mathsf{C}}(*)$, we obtain that ψ is valid too and therefore $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \psi$ as $\mathcal{H}_{\mathsf{C}}$ is a subsystem of $\mathcal{H}_{\mathsf{C}}(*)$ and $\mathcal{H}_{\mathsf{C}}$ is complete by Theorem 4.3. By propositional reasoning, we get that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi$.

To show that every formula φ has a provably equivalent Boolean combination of core formulae, we heavily rely on Corollary 5.5. The proof is by simple induction on the number of occurrences of $*$ in φ that are not involved in the definition of some core formula of the form $\mathtt{size} \geqslant \beta$. For the base case, when φ has no occurrence of the separating conjunction, $\mathtt{x} = \mathtt{y}$ and $\mathtt{x} \hookrightarrow \mathtt{y}$ are already core formulae, and $\mathtt{emp}$ is logically equivalent to $\neg \mathtt{size} \geqslant 1$.

Before performing the induction step, let us observe that in $\mathcal{H}_{\mathsf{C}}(*)$, the replacement of provably equivalent formulae holds true, which is stated as follows:

R0 Let φ, φ' and ψ be formulae of $\mathsf{SL}(*, \mathtt{alloc})$ such that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi \Leftrightarrow \varphi'$. Then,

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \psi[\varphi]_\rho \Rightarrow \psi[\varphi']_\rho$$

Above, $\psi[\varphi]_\rho$ refers to the formula ψ in which the subformula at the occurrence ρ (in the standard sense) is replaced by φ. (φ and φ' are therefore placed at the same occurrence.)

To prove **R0**, we first note that the following rules can be shown admissible in $\mathcal{H}_{\mathsf{C}}(*)$:

$$\frac{\varphi \Leftrightarrow \varphi'}{\neg\varphi \Leftrightarrow \neg\varphi'} \qquad \frac{\varphi \Leftrightarrow \varphi'}{\varphi \vee \psi \Leftrightarrow \varphi' \vee \psi} \qquad \frac{\varphi \Leftrightarrow \varphi'}{\varphi \wedge \psi \Leftrightarrow \varphi' \wedge \psi}$$

Admissibility of such rules is a direct consequence of the presence of axioms and modus ponens for the propositional calculus. As a consequence of the presence of the rule $*$**-Intro** in $\mathcal{H}_{\mathsf{C}}(*)$, the rule below is also admissible:

$$\frac{\varphi \Leftrightarrow \varphi'}{\varphi * \psi \Leftrightarrow \varphi' * \psi}$$

Consequently, by structural induction on ψ, one can conclude that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi \Leftrightarrow \varphi'$ implies $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \psi[\varphi]_\rho \Rightarrow \psi[\varphi']_\rho$ (the axiom $\mathbf{(A_7^*)}$ needs to be used here).

Assume that φ is a formula in $\mathsf{SL}(*, \mathtt{alloc})$ with $n+1$ occurrences of the separating conjunction not involved in the definition of some $\mathtt{size} \geqslant \beta$ ($n \geqslant 0$). Let ψ be a subformula of φ (at the occurrence ρ) of the form $\psi_1 * \psi_2$ such that ψ_1 and ψ_2 are Boolean combinations of core formulae, in $\mathsf{Bool}(\mathsf{Core}(\mathtt{X}, \alpha_1))$ and $\mathsf{Bool}(\mathsf{Core}(\mathtt{X}, \alpha_2))$. By pure propositional reasoning, one can show that there are formulae in disjunctive normal form $\psi_1^1 \vee \cdots \vee \psi_1^{n_1}$ and $\psi_2^1 \vee \cdots \vee \psi_2^{n_2}$ such that $\vdash_{\mathcal{H}_{\mathsf{C}}} \psi_i \Leftrightarrow \psi_i^1 \vee \cdots \vee \psi_i^{n_i}$ for $i \in \{1, 2\}$ and moreover, all the ψ_i^j's are core types in $\mathsf{CoreTypes}(\mathtt{X}, \max(\mathrm{card}(\mathtt{X}), \alpha_1, \alpha_2))$. Again, by using propositional reasoning but this time using also the axiom $\mathbf{(I_9^*)}$ for distributivity, we have

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \psi_1 * \psi_2 \Leftrightarrow \bigvee_{j_1 \in [1,n_1], j_2 \in [1,n_2]} \psi_1^{j_1} * \psi_2^{j_2}.$$

We now rely on Corollary 5.5 and derive that there is a conjunction of core formulae ψ^{j_1,j_2} in $\mathsf{Conj}(\mathsf{Core}(\mathtt{X}, 2\max(\mathrm{card}(\mathtt{X}), \alpha_1, \alpha_2)))$ such that $\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \psi_1^{j_1} * \psi_2^{j_2} \Leftrightarrow \psi^{j_1,j_2}$. By propositional reasoning, we get

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \psi_1 * \psi_2 \Leftrightarrow \bigvee_{j_1 \in [1,n_1], j_2 \in [1,n_2]} \psi^{j_1,j_2}.$$

$\mathbf{(A^{-\!\circledast}_{21})}$ $(\mathtt{size} = 1 \wedge \bigwedge_{\mathtt{x}\in\mathtt{X}} \neg\mathtt{alloc}(\mathtt{x})) \mathrel{-\!\!\circledast} \top$ $\blacktriangleleft[\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}]$

$\mathbf{(A^{-\!\circledast}_{22})}$ $\neg\mathtt{alloc}(\mathtt{x}) \Rightarrow ((\mathtt{x} \hookrightarrow \mathtt{y} \wedge \mathtt{size} = 1) \mathrel{-\!\!\circledast} \top)$

$\mathbf{(A^{-\!\circledast}_{23})}$ $\neg\mathtt{alloc}(\mathtt{x}) \Rightarrow ((\mathtt{alloc}(\mathtt{x}) \wedge \mathtt{size} = 1 \wedge \bigwedge_{\mathtt{y}\in\mathtt{X}} \neg\mathtt{x} \hookrightarrow \mathtt{y}) \mathrel{-\!\!\circledast} \top)$ $\blacktriangleleft[\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}]$

$*$**-Adj**: $\dfrac{\varphi * \psi \Rightarrow \chi}{\varphi \Rightarrow (\psi \mathrel{-\!\!*} \chi)}$ $\qquad$ $\mathrel{-\!\!*}$**-Adj**: $\dfrac{\varphi \Rightarrow (\psi \mathrel{-\!\!*} \chi)}{\varphi * \psi \Rightarrow \chi}$

Figure 7: Additional axioms and rules for handling the separating implication.

Consequently (thanks to the property **R0**), we obtain

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*)} \varphi \Leftrightarrow \varphi[\bigvee_{j_1\in[1,n_1],j_2\in[1,n_2]} \psi^{j_1,j_2}]_\rho$$

Note that the right-hand side formula has n occurrences of the separating conjunction that are not involved in the definition of some core formula of the form $\mathtt{size} \geqslant \beta$. The induction hypothesis applies, which concludes the proof. □

6. A constructive elimination of $\mathrel{-\!\!*}$ leading to full completeness

In order to obtain the final proof system $\mathcal{H}_{\mathsf{C}}(*, \mathrel{-\!\!*})$, we add the axioms and rules from Figure 7 to the proof system $\mathcal{H}_{\mathsf{C}}(*)$. These new axioms and rules are dedicated to the separating implication. The axioms involving $\mathrel{-\!\!\circledast}$ (kind of dual of $\mathrel{-\!\!*}$, introduced in Section 2) express that it is always possible to extend a given heap with an extra cell, and that the address and the content of this cell can be fixed arbitrarily (provided it is not already allocated). The adjunction rules $*$**-Adj** and $\mathrel{-\!\!*}$**-Adj** are from the Hilbert-style axiomatisation of Boolean BI [GLW06, Section 2]. One can observe that, in $\mathcal{H}_{\mathsf{C}}(*, \mathrel{-\!\!*})$, the axioms $\mathbf{(I^*_9)}$, $\mathbf{(I^*_{10})}$ and $\mathbf{(I^*_{12})}$ of $\mathcal{H}_{\mathsf{C}}(*)$ are derivable.

Lemma 6.1. *The axioms $\mathbf{(I^*_9)}$, $\mathbf{(I^*_{10})}$ and $\mathbf{(I^*_{12})}$ are derivable in $\mathcal{H}_{\mathsf{C}}(*, \mathrel{-\!\!*})$.*

The derivations of $\mathbf{(I^*_9)}$, $\mathbf{(I^*_{10})}$ and $\mathbf{(I^*_{12})}$ that lead to Lemma 6.1 are given in Appendix C.

Fundamentally, $\mathcal{H}_{\mathsf{C}}(*, \mathrel{-\!\!*})$ enjoys the $\mathrel{-\!\!*}$ elimination property, as shown below. Actually, we state the property with the help of $\mathrel{-\!\!\circledast}$ as we find the related statements and developments more intuitive.

Lemma 6.2. *Let $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$ and $\alpha \geqslant \mathrm{card}(\mathtt{X})$. Let φ and ψ in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$. There is a conjunction $\chi \in \mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \alpha))$ such that $\vdash_{\mathcal{H}_{\mathsf{C}}(*,\mathrel{-\!\!*})} (\varphi \mathrel{-\!\!\circledast} \psi) \Leftrightarrow \chi$.*

Structure of the proof of Lemma 6.2. In the proof of Lemma 6.2, the formula χ is explicitly constructed from φ and ψ, following a pattern analogous to the construction of $\langle * \rangle(.,.)$ in Figure 6 (see forthcoming Figure 8). The derivation of the equivalence $(\varphi \mathrel{-\!\!\circledast} \psi) \Leftrightarrow \chi$ is shown as follows. First, the formulae $\chi * \varphi \Rightarrow \psi$ and $\neg\chi * \varphi \Rightarrow \neg\psi$ are shown valid (by using semantical means). As $\mathcal{H}_{\mathsf{C}}(*)$ is complete for $\mathsf{SL}(*, \mathtt{alloc})$, it is a subsystem of $\mathcal{H}_{\mathsf{C}}(*, \mathrel{-\!\!*})$, and the formulae φ, ψ and χ are Boolean combinations of core formulae, we get $\vdash_{\mathcal{H}_{\mathsf{C}}(*,\mathrel{-\!\!*})} \chi * \varphi \Rightarrow \psi$ and $\vdash_{\mathcal{H}_{\mathsf{C}}(*,\mathrel{-\!\!*})} \neg\chi * \varphi \Rightarrow \neg\psi$. The latter theorem leads to $\vdash_{\mathcal{H}_{\mathsf{C}}(*,\mathrel{-\!\!*})} (\varphi \mathrel{-\!\!\circledast} \psi) \Rightarrow \chi$ by using the definition of $\mathrel{-\!\!\circledast}$ and the rule $*$**-Adj**. For the other direction, in order to show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*,\mathrel{-\!\!*})} \chi \Rightarrow (\varphi \mathrel{-\!\!\circledast} \psi)$ holds, we take advantage of the admissibility of the theorem $\mathbf{(I^{-\!*}_{6.3.9})}$ (see Lemma 6.3) for which an instance is $(\varphi \mathrel{-\!\!\circledast} \top) \wedge (\varphi \mathrel{-\!\!*} \psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} (\top \wedge \psi))$. From $\vdash_{\mathcal{H}_{\mathsf{C}}(*,\mathrel{-\!\!*})} \chi * \varphi \Rightarrow \psi$ and by $*$**-Adj** we

have $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \chi \Rightarrow (\varphi \mathrel{-\!\!*} \psi)$. Therefore, the main technical development lies in the proof of $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \chi \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$, which allows us to take advantage of $\mathbf{(I^{-\!\!*}_{6.3.9})}$, and leads to $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \chi \Rightarrow (\varphi \mathrel{-\!\!\circledast} \psi)$ by propositional reasoning.

In order to formalise the proof of Lemma 6.2 sketched above, we start by establishing several admissible axioms and rules (Lemma 6.3). Afterwards, we define the formula χ and show the validity of $\chi * \varphi \Rightarrow \psi$ and $\neg\chi * \varphi \Rightarrow \neg\psi$ (Lemma 6.4). Then, come the final bits of the proof of Lemma 6.2 (see page 35).

Lemma 6.3. *The following rules and axioms are admissible in* $\mathcal{H}_{\mathsf{C}}(*,-\!\!*)$*:*

$\mathbf{(I^{-\!\!*}_{6.3.1})}$ $\bot \mathrel{-\!\!\circledast} \varphi \Rightarrow \bot$

$\mathbf{(I^{-\!\!*}_{6.3.2})}$ $\varphi \mathrel{-\!\!\circledast} \bot \Rightarrow \bot$

$\mathbf{(I^{-\!\!*}_{6.3.3})}$ $\varphi * (\varphi \mathrel{-\!\!*} \psi) \Rightarrow \psi$

$\mathbf{(I^{-\!\!*}_{6.3.4})}$ $\dfrac{\varphi \Rightarrow \psi}{\varphi \mathrel{-\!\!\circledast} \chi \Rightarrow \psi \mathrel{-\!\!\circledast} \chi}$

$\mathbf{(I^{-\!\!*}_{6.3.5})}$ $\dfrac{\varphi \Rightarrow \psi}{\chi \mathrel{-\!\!\circledast} \varphi \Rightarrow \chi \mathrel{-\!\!\circledast} \psi}$

$\mathbf{(I^{-\!\!*}_{6.3.6})}$ $\varphi \mathrel{-\!\!\circledast} (\psi \mathrel{-\!\!\circledast} \chi) \;\Leftrightarrow\; (\varphi * \psi) \mathrel{-\!\!\circledast} \chi$

$\mathbf{(I^{-\!\!*}_{6.3.7})}$ $(\varphi \vee \psi) \mathrel{-\!\!\circledast} \chi \;\Leftrightarrow\; (\varphi \mathrel{-\!\!\circledast} \chi) \vee (\psi \mathrel{-\!\!\circledast} \chi)$

$\mathbf{(I^{-\!\!*}_{6.3.8})}$ $\chi \mathrel{-\!\!\circledast} (\varphi \vee \psi) \;\Leftrightarrow\; (\chi \mathrel{-\!\!\circledast} \varphi) \vee (\chi \mathrel{-\!\!\circledast} \psi)$

$\mathbf{(I^{-\!\!*}_{6.3.9})}$ $(\varphi \mathrel{-\!\!\circledast} \psi) \wedge (\varphi \mathrel{-\!\!*} \chi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \psi \wedge \chi)$

$\mathbf{(I^{-\!\!*}_{6.3.10})}$ $\mathtt{x} = \mathtt{y} \wedge (\varphi \mathrel{-\!\!\circledast} \psi) \Rightarrow (\varphi \wedge \mathtt{x} = \mathtt{y} \mathrel{-\!\!\circledast} \psi)$

$\mathbf{(I^{-\!\!*}_{6.3.11})}$ $\mathtt{x} \neq \mathtt{y} \wedge (\varphi \mathrel{-\!\!\circledast} \psi) \Rightarrow (\varphi \wedge \mathtt{x} \neq \mathtt{y} \mathrel{-\!\!\circledast} \psi)$

$\mathbf{(I^{-\!\!*}_{6.3.12})}$ $(\varphi_{\mathtt{size}} \wedge \bigwedge_{\mathtt{x} \in \mathtt{X}} \neg \mathtt{alloc}(\mathtt{x})) \mathrel{-\!\!\circledast} \top$,

where, in axiom $\mathbf{(I^{-\!\!*}_{6.3.12})}$, $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$ *and* $\varphi_{\mathtt{size}}$ *is a satisfiable conjunction of literals of the form* $\mathtt{size} \geqslant \beta_1$ *or* $\neg\mathtt{size} \geqslant \beta_2$.

The proof of Lemma 6.3 can be found in Appendix D.

Let φ and ψ be two satisfiable core types in $\mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \alpha))$. Following the developments of Section 5, we define a formula $\langle \mathtt{sep} \rangle(\varphi, \psi)$ in $\mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \alpha))$, for which we show that $\varphi \mathrel{-\!\!\circledast} \psi \Leftrightarrow \langle \mathtt{sep} \rangle(\varphi, \psi)$ is provable in $\mathcal{H}_{\mathsf{C}}(*,-\!\!*)$. The formula $\langle \mathtt{sep} \rangle(\varphi, \psi)$ is defined in Figure 8.

Lemma 6.4. *Let* $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$, $\alpha \geqslant \mathrm{card}(\mathtt{X})$ *and* φ, ψ *be satisfiable core types in* $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$. *The formulae* $\langle \mathtt{sep} \rangle(\varphi, \psi) * \varphi \Rightarrow \psi$ *and* $(\neg\langle \mathtt{sep} \rangle(\varphi, \psi)) * \varphi \Rightarrow \neg\psi$ *are valid.*

Before presenting the proof for Lemma 6.4, let us observe that since we aim at proving the derivability of $\varphi \mathrel{-\!\!\circledast} \psi \Leftrightarrow \langle \mathtt{sep} \rangle(\varphi, \psi)$ in $\mathcal{H}_{\mathsf{C}}(*,-\!\!*)$, the validity of the formula $(\neg\langle \mathtt{sep} \rangle(\varphi, \psi)) * \varphi \Rightarrow \neg\psi$ should not surprise the reader. Indeed, by replacing $\langle \mathtt{sep} \rangle(\varphi, \psi)$ with $\varphi \mathrel{-\!\!\circledast} \psi$ we obtain $(\neg(\varphi \mathrel{-\!\!\circledast} \psi)) * \varphi \Rightarrow \neg\psi$ which, unfolding the definition of $\mathrel{-\!\!\circledast}$, is equivalent to the valid formula $(\varphi \mathrel{-\!\!*} \neg\psi) * \varphi \Rightarrow \neg\psi$ (see $\mathbf{(I^{-\!\!*}_{6.3.3})}$ in Lemma 6.3). On the other hand, the fact that $\langle \mathtt{sep} \rangle(\varphi, \psi) * \varphi \Rightarrow \psi$ is valid can be puzzling at first, as the formula $(\varphi \mathrel{-\!\!\circledast} \psi) * \varphi \Rightarrow \psi$ is not valid (in general). In its essence, Lemma 6.4 shows that $(\varphi \mathrel{-\!\!\circledast} \psi) * \varphi \Rightarrow \psi$ is valid whenever φ and ψ are restricted to core types.

Below, we prove that $\langle \mathtt{sep} \rangle(\varphi, \psi) * \varphi \Rightarrow \psi$ and $(\neg\langle \mathtt{sep} \rangle(\varphi, \psi)) * \varphi \Rightarrow \neg\psi$ are valid, thus establishing Lemma 6.4. Notice that the proof is carried out through semantical arguments. Since φ, ψ and $\langle \mathtt{sep} \rangle(\varphi, \psi)$ are conjunctions of literals built from core formulae, derivability of these two tautologies in $\mathcal{H}_{\mathsf{C}}(*,-\!\!*)$ follows from the completeness of $\mathcal{H}_{\mathsf{C}}(*)$ (Theorem 5.6).

Validity of $\langle \mathtt{sep} \rangle(\varphi, \psi) * \varphi \Rightarrow \psi$. If $\langle \mathtt{sep} \rangle(\varphi, \psi) * \varphi$ is inconsistent, then $\langle \mathtt{sep} \rangle(\varphi, \psi) * \varphi \Rightarrow \psi$ is straightforwardly valid. Below, we assume that $\langle \mathtt{sep} \rangle(\varphi, \psi) * \varphi$ is satisfiable. In particular, none of the conditions depicted in Figure 8 that result in $\langle \mathtt{sep} \rangle(\varphi, \psi)$ having a literal $\mathtt{x} \neq \mathtt{x}$ applies. Let $(s, h) \models \langle \mathtt{sep} \rangle(\varphi, \psi) * \varphi$. Therefore, there are two disjoint heaps h_1 and h_2 such that $h = h_1 + h_2$, $(s, h_1) \models \langle \mathtt{sep} \rangle(\varphi, \psi)$ and $(s, h_2) \models \varphi$. We show that (s, h) satisfies each

$$\bigwedge \left\{ \mathtt{x} \sim \mathtt{y} \subseteq_{\mathsf{Lt}} \{\varphi \mid \psi\} \,\middle|\, \sim \in \{=, \neq\} \right\} \qquad \wedge \bigwedge \left\{ \mathtt{alloc(x)} \,\middle|\, \begin{array}{r} \neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi \\ \mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$

$$\wedge \bigwedge \{\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \psi\} \qquad \wedge \bigwedge \left\{ \neg\mathtt{alloc(x)} \,\middle|\, \mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi \right\}$$

$$\wedge \bigwedge \{\neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi\} \qquad \wedge \bigwedge \left\{ \mathtt{x} \hookrightarrow \mathtt{y} \,\middle|\, \begin{array}{r} \neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi \\ \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$

$$\wedge \bigwedge \left\{ \mathtt{x} \neq \mathtt{x} \,\middle|\, \begin{array}{r} \mathtt{alloc(x)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi \\ \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi \end{array} \right\} \qquad \wedge \bigwedge \left\{ \mathtt{size} \geqslant \beta_2 + 1 \dot{-} \beta_1 \,\middle|\, \begin{array}{r} \neg\mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi \\ \mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$

$$\wedge \bigwedge \left\{ \mathtt{x} \neq \mathtt{x} \,\middle|\, \begin{array}{r} \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi \\ \neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi \end{array} \right\} \qquad \wedge \bigwedge \left\{ \neg\mathtt{size} \geqslant \beta_2 \dot{-} \beta_1 \,\middle|\, \begin{array}{r} \mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi \\ \neg\mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$

$$\wedge \bigwedge \left\{ \mathtt{x} \neq \mathtt{x} \,\middle|\, \begin{array}{r} \mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi \\ \neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$

Figure 8: The formula $\langle \mathtt{sep} \rangle(\varphi, \psi)$.

literal L in ψ. We perform a simple case analysis on the shape of L. Notice that, below, we have $\mathtt{x}, \mathtt{y} \in \mathtt{X}$ and $\beta_2 \in [0, \alpha]$, as ψ is a core type in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$.

case: $L = \mathtt{x} \sim \mathtt{y}$**, where** $\sim \in \{=, \neq\}$**:** By definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, $\mathtt{x} \sim \mathtt{y} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$ and so $(s, h_1) \models \mathtt{x} \sim \mathtt{y}$. We conclude that $s(\mathtt{x}) \sim s(\mathtt{y})$, and thus $(s, h) \models \mathtt{x} \sim \mathtt{y}$.

case: $L = \mathtt{alloc(x)}$**:** If $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$, then $(s, h_2) \models \mathtt{alloc(x)}$, which implies $s(\mathtt{x}) \in \mathrm{dom}(h)$ directly from $h_2 \sqsubseteq h$. Thus, $(s, h) \models \mathtt{alloc(x)}$. Otherwise, if $\mathtt{alloc(x)} \not\subseteq_{\mathsf{Lt}} \varphi$ then, since φ is a core type in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, we have $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$. By definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, we derive that $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. So, $(s, h_1) \models \mathtt{alloc(x)}$ and thus, by $h_1 \sqsubseteq h$, $s(\mathtt{x}) \in \mathrm{dom}(h)$. We conclude that $(s, h) \models \mathtt{alloc(x)}$.

case: $L = \neg\mathtt{alloc(x)}$**:** In this case, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, we have $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, which implies $(s, h_1) \models \neg\mathtt{alloc(x)}$. *Ad absurdum*, suppose $(s, h_2) \models \mathtt{alloc(x)}$. Since φ is a core type in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, we conclude that $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$. However, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, this implies $\mathtt{x} \neq \mathtt{x} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, which contradicts the fact that $\langle \mathtt{sep} \rangle(\varphi, \psi)$ is satisfiable. Thus, $(s, h_2) \models \neg\mathtt{alloc(x)}$, which implies $s(\mathtt{x}) \notin \mathrm{dom}(h_2)$. From $h = h_1 + h_2$ and $s(\mathtt{x}) \notin \mathrm{dom}(h_1)$ we conclude that $s(\mathtt{x}) \notin \mathrm{dom}(h)$. So, $(s, h) \models \neg\mathtt{alloc(x)}$.

case: $L = \mathtt{x} \hookrightarrow \mathtt{y}$**:** If $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$, then $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$ holds by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$. So, $h_1(s(\mathtt{x})) = s(\mathtt{y})$ and, from $h_1 \sqsubseteq h$ we conclude that $(s, h) \models \mathtt{x} \hookrightarrow \mathtt{y}$. Otherwise, let us assume that $\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$. *Ad absurdum*, suppose $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$. Then, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, we derive $\mathtt{x} \neq \mathtt{x} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. However, this contradicts the satisfiability of $\langle \mathtt{sep} \rangle(\varphi, \psi)$. Therefore, $\neg\mathtt{x} \hookrightarrow \mathtt{y} \not\subseteq_{\mathsf{Lt}} \varphi$. Since φ is a core type, this implies $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$, and therefore $h_2(s(\mathtt{x})) = s(\mathtt{y})$. From $h_2 \sqsubseteq h$ we conclude that $(s, h) \models \mathtt{x} \hookrightarrow \mathtt{y}$.

case: $L = \neg\mathtt{x} \hookrightarrow \mathtt{y}$**:** By definition of $\langle \mathtt{sep} \rangle(\mathtt{x}, \mathtt{y})$, we have $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\mathtt{x}, \mathtt{y})$, which implies that if $s(\mathtt{x}) \in \mathrm{dom}(h_1)$ then $h_1(s(\mathtt{x})) \neq s(\mathtt{y})$. *Ad absurdum*, suppose $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$. Then, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, we derive $\mathtt{x} \neq \mathtt{x} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. However, this contradicts the satisfiability of $\langle \mathtt{sep} \rangle(\varphi, \psi)$. Therefore $\mathtt{x} \hookrightarrow \mathtt{y} \not\subseteq_{\mathsf{Lt}} \varphi$ and, since φ is a core type, $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$. So, if $s(\mathtt{x}) \in \mathrm{dom}(h_2)$ then $h_2(s(\mathtt{x})) \neq s(\mathtt{y})$. By $h = h_1 + h_2$ and the fact that $h_1(s(\mathtt{x})) \neq s(\mathtt{y})$, we conclude that $(s, h) \models \neg\mathtt{x} \hookrightarrow \mathtt{y}$.

case: $L = \mathtt{size} \geqslant \beta_2$**:** If $\mathtt{size} \geqslant \alpha \subseteq_{\mathsf{Lt}} \varphi$, then $\mathrm{card}(\mathrm{dom}(h)) \geqslant \mathrm{card}(\mathrm{dom}(h_2)) \geqslant \alpha$, by $h_2 \sqsubseteq h$. As $\beta_2 \in [0, \alpha]$, this implies $(s, h) \models \mathtt{size} \geqslant \beta_2$. Otherwise, assume $\mathtt{size} \geqslant \alpha \not\subseteq_{\mathsf{Lt}} \varphi$.

In particular, since φ is in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, this implies that $\max_{\mathtt{size}}(\varphi) < \alpha$ and

$$\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \wedge \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \ \subseteq_{\mathsf{Lt}} \ \varphi.$$

We have $\mathrm{card}(\mathrm{dom}(h_2)) = \max_{\mathtt{size}}(\varphi)$. If $\max_{\mathtt{size}}(\varphi) \geqslant \beta_2$, then from $h_2 \sqsubseteq h$ we conclude that $(s,h) \models \mathtt{size} \geqslant \beta_2$. Otherwise, let us assume $\beta_2 > \max_{\mathtt{size}}(\varphi)$. By definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, we conclude that $\mathtt{size} \geqslant \beta_2 + 1 \dot{-} (\max_{\mathtt{size}}(\varphi) + 1) \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. Together with $\beta_2 > \max_{\mathtt{size}}(\varphi)$, this implies $\mathrm{card}(\mathrm{dom}(h_1)) \geqslant \beta_2 - \max_{\mathtt{size}}(\varphi)$. With $\mathrm{card}(\mathrm{dom}(h_2)) = \max_{\mathtt{size}}(\varphi)$ and $h = h_1 + h_2$, this implies $(s,h) \models \mathtt{size} \geqslant \beta_2$.

case: $L = \neg\mathtt{size} \geqslant \beta_2$**:** *Ad absurdum*, suppose that $\mathtt{size} \geqslant \alpha \subseteq_{\mathsf{Lt}} \varphi$. Then, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$ we have $\neg\mathtt{size} \geqslant \beta_2 \dot{-} \alpha \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. However, since $\beta_2 \in [0, \alpha]$, this means that $\neg\mathtt{size} \geqslant 0 \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, which contradicts the satisfiability of $\langle \mathtt{sep} \rangle(\varphi, \psi)$. Therefore, $\mathtt{size} \geqslant \alpha \not\subseteq_{\mathsf{Lt}} \varphi$. As φ is in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, we derive $\max_{\mathtt{size}}(\varphi) < \alpha$ and

$$\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \wedge \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \ \subseteq_{\mathsf{Lt}} \ \varphi.$$

We conclude that $\mathrm{card}(\mathrm{dom}(h_2)) \leqslant \max_{\mathtt{size}}(\varphi)$. From $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \subseteq_{\mathsf{Lt}} \varphi$ and by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, we conclude that

$$\neg\mathtt{size} \geqslant \beta_2 \dot{-} \max_{\mathtt{size}}(\varphi) \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi).$$

If $\beta_2 \leqslant \max_{\mathtt{size}}(\varphi)$, then $\neg\mathtt{size} \geqslant 0 \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, which contradicts the satisfiability of $\langle \mathtt{sep} \rangle(\varphi, \psi)$. Therefore, $\beta_2 > \max_{\mathtt{size}}(\varphi)$. So, $\mathrm{card}(\mathrm{dom}(h_1)) < \beta_2 - \max_{\mathtt{size}}(\varphi)$. Together with $\mathrm{card}(\mathrm{dom}(h_2)) \leqslant \max_{\mathtt{size}}(\varphi)$ and $h = h_1 + h$, we conclude that $\mathrm{card}(\mathrm{dom}(h)) < \beta_2$, and thus $(s,h) \models \neg\mathtt{size} \geqslant \beta_2$. □

Validity of $(\neg\langle \mathtt{sep} \rangle(\varphi, \psi)) * \varphi \Rightarrow \neg\psi$. Let us assume $(s,h) \models (\neg\langle \mathtt{sep} \rangle(\varphi, \psi)) * \varphi$. Consequently, there is a literal L of $\langle \mathtt{sep} \rangle(\varphi, \psi)$ such that $(s,h) \models (\neg L) * \varphi$ holds. We show that $(s,h) \models \neg\psi$. Let h_1 and h_2 be two disjoint heaps such that $h = h_1 + h_2$, $(s, h_1) \models \neg L$ and $(s, h_2) \models \varphi$. We perform a case analysis on the shape of L. As in the previous part of the proof, recall that $\mathtt{x}, \mathtt{y} \in \mathtt{X}$ and $\beta_1, \beta_2 \in [0, \alpha]$.

case: $L = \mathtt{x} \neq \mathtt{x}$**:** Since φ and ψ are satisfiable, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, the fact that $\mathtt{x} \neq \mathtt{x} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$ implies that one of the following three cases holds:

1: $\mathtt{alloc}(\mathtt{x}) \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$ and $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi$.
From $\mathtt{alloc}(\mathtt{x}) \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$ and $h_2 \sqsubseteq h$, we have $s(\mathtt{x}) \in \mathrm{dom}(h)$ and $h(s(\mathtt{x})) \neq s(\mathtt{y})$. Thus $(s,h) \not\models \mathtt{x} \hookrightarrow \mathtt{y}$, and so, by $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi$, $(s,h) \models \neg\psi$.

2: $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$ and $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi$.
From $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$ and $h_2 \sqsubseteq h$, $h(s(\mathtt{x})) = s(\mathtt{y})$. Thus $(s,h) \models \mathtt{x} \hookrightarrow \mathtt{y}$ and so, by $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi$, $(s,h) \models \neg\psi$.

3: $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi$ and $\neg\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \psi$.
From $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi$ and $h_2 \sqsubseteq h$, $s(\mathtt{x}) \in \mathrm{dom}(h)$. Thus $(s,h) \models \mathtt{alloc}(\mathtt{x})$ and so, by $\neg\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \psi$, $(s,h) \models \neg\psi$.

case: $L = \mathtt{x} \sim \mathtt{y}$**, where** $\sim \in \{=, \neq\}$**:** In this case, since $(s, h_1) \models \neg L$, then we have $(s,h) \models \neg L$. Now, it cannot be that $L \subseteq_{\mathsf{Lt}} \varphi$, as it would imply $(s,h) \models L$, which is contradictory. Therefore, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, we must have $L \subseteq_{\mathsf{Lt}} \psi$. This implies $(s,h) \models \neg\psi$.

case: $L = \mathtt{alloc}(\mathtt{x})$**:** By definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, $\neg\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi$ and $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \psi$. From $(s, h_1) \models \neg\mathtt{alloc}(\mathtt{x})$ we conclude that $s(\mathtt{x}) \notin \mathrm{dom}(h_1)$. By $\neg\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi$, $s(\mathtt{x}) \notin \mathrm{dom}(h_2)$. By $h = h_1 + h_2$, $s(\mathtt{x}) \notin \mathrm{dom}(h)$. As $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \psi$, $(s,h) \models \neg\psi$.

case: $L = \neg\mathtt{alloc}(\mathtt{x})$**:** As $(s, h_1) \models \neg L$, we have $s(\mathtt{x}) \in \mathrm{dom}(h_1)$. According to the definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, either $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi$ or $\neg\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \psi$. The first case

cannot hold, as it implies $s(\mathtt{x}) \in \mathrm{dom}(h_2)$ which contradicts the fact that h_1 and h_2 are disjoint. In the second case, from $s(\mathtt{x}) \in \mathrm{dom}(h_1)$ and $h_1 \sqsubseteq h$, we have $(s,h) \models \mathtt{alloc(x)}$. So, $(s,h) \models \neg\psi$.

case: $L = \mathtt{x} \hookrightarrow \mathtt{y}$**:** Then by definition of $\langle \mathtt{sep} \rangle(\varphi,\psi)$, $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$ and $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi$. From $(s,h_1) \models \neg L$, if $s(\mathtt{x}) \in \mathrm{dom}(h_1)$ then $h_1(s(\mathtt{x})) \neq s(\mathtt{y})$. As $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$, $s(\mathtt{x}) \notin \mathrm{dom}(h_2)$ and therefore, by $h = h_1 + h_2$, $h(s(\mathtt{x})) \neq s(\mathtt{y})$. From $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi$, we conclude that $(s,h) \models \neg\psi$.

case: $L = \neg\mathtt{x} \hookrightarrow \mathtt{y}$**:** Then, by definition of $\langle \mathtt{sep} \rangle(\varphi,\psi)$, $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi$. From $(s,h_1) \models \neg L$ and $h_1 \sqsubseteq h$, we derive $h(s(\mathtt{x})) = s(\mathtt{y})$. From $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi$, we derive $(s,h) \models \neg\psi$.

case: $L = \mathtt{size} \geqslant \beta_2 + 1 \dot{-} \beta_1$**, where** $\mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi$ **and** $\neg\mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi$**:** Since it holds that $(s,h_1) \models \neg L$ and $(s,h_2) \models \varphi$, we derive (respectively) $\mathrm{card}(\mathrm{dom}(h_1)) \leqslant \beta_2 \dot{-} \beta_1$ and $\mathrm{card}(\mathrm{dom}(h_2)) < \beta_1$. From $h = h_1 + h_2$, we conclude that $\mathrm{card}(\mathrm{dom}(h)) < \beta_2$. From $\mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi$, we derive $(s,h) \models \neg\psi$.

case: $L = \neg\mathtt{size} \geqslant \beta_2 \dot{-} \beta_1$**, where** $\neg\mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi$ **and** $\mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi$**:** Since we have $(s,h_1) \models \neg L$ and $(s,h_2) \models \varphi$, we conclude that $\mathrm{card}(\mathrm{dom}(h_1)) \geqslant \beta_2 \dot{-} \beta_1$ and $\mathrm{card}(\mathrm{dom}(h_2)) \geqslant \beta_1$. So, $h = h_1 + h_2$ implies $\mathrm{card}(\mathrm{dom}(h)) \geqslant \beta_2$. By $\neg\mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi$, we derive $(s,h) \models \neg\psi$. □

We are now ready to tackle the proof of Lemma 6.2.

Proof of Lemma 6.2. As in the statement of the lemma, let us consider $\mathtt{X} \subseteq_{\mathsf{fin}} \mathsf{VAR}$ and $\alpha \geqslant \mathrm{card}(\mathtt{X})$, and two core types φ and ψ in $\mathsf{CoreTypes}(\mathtt{X},\alpha)$. We want to show that there is a conjunction $\chi \in \mathsf{Conj}(\mathsf{Core}(\mathtt{X},\alpha))$ such that $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} (\varphi \mathbin{-\!\!\circledast} \psi) \Leftrightarrow \chi$.

First of all, if φ or ψ is unsatisfiable, then $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \varphi \mathbin{-\!\!\circledast} \psi \Rightarrow \bot$ by using Lemma 4.1 and the admissible axioms $\mathbf{(I^{-\!\!*}_{6.3.4})}$ and $\mathbf{(I^{-\!\!*}_{6.3.5})}$ from Lemma 6.3. Therefore, in this case, it is enough to take χ equal to $\neg\mathtt{x} = \mathtt{x}$ to complete the proof. Otherwise, let us assume that φ and ψ are satisfiable. We consider $\chi \stackrel{\text{def}}{=} \langle \mathtt{sep} \rangle(\varphi,\psi)$ (see Figure 8), and show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} (\varphi \mathbin{-\!\!\circledast} \psi) \Leftrightarrow \langle \mathtt{sep} \rangle(\varphi,\psi)$. We derive each implication separately.

($\Rightarrow$): Given Lemma 6.4, the proof of $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \varphi \mathbin{-\!\!\circledast} \psi \Rightarrow \langle \mathtt{sep} \rangle(\varphi,\psi)$ is straightforward:

1	$\neg\langle \mathtt{sep} \rangle(\varphi,\psi) * \varphi \Rightarrow \neg\psi$	Lemma 6.4, Theorem 5.6
2	$\neg\langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow (\varphi \mathbin{-\!\!*} \neg\psi)$	$*$**-Adj**, 1
3	$\neg(\varphi \mathbin{-\!\!*} \neg\psi) \Rightarrow \langle \mathtt{sep} \rangle(\varphi,\psi)$	PC, 2
4	$(\varphi \mathbin{-\!\!\circledast} \psi) \Rightarrow \langle \mathtt{sep} \rangle(\varphi,\psi)$	Def. of $-\!\!\circledast$, 3

($\Leftarrow$): Let us now show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathbin{-\!\!\circledast} \psi$. First, let us note that, since $\langle \mathtt{sep} \rangle(\varphi,\psi) * \varphi \Rightarrow \psi$ is valid (Lemma 6.4), it is derivable in $\mathcal{H}_{\mathsf{C}}(*)$ (Theorem 5.6), and therefore, by the rule $*$**-Adj**, $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathbin{-\!\!*} \psi$. From that, it follows that it is enough to show that $\langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathbin{-\!\!\circledast} \top$ is derivable in $\mathcal{H}_{\mathsf{C}}(*,-\!\!*)$. Indeed, from $\langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathbin{-\!\!\circledast} \top$ and $\langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathbin{-\!\!*} \psi$, we get, by $\mathbf{(I^{-\!\!*}_{6.3.9})}$, that $\langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathbin{-\!\!\circledast} \psi$ is derivable too.

Thus, let us prove that $\langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathbin{-\!\!\circledast} \top$ is derivable. If $\langle \mathtt{sep} \rangle(\varphi,\psi)$ is unsatisfiable, then from the completeness of $\mathcal{H}_{\mathsf{C}}$ with respect to Boolean combinations of core formulae (Theorem 4.3), we conclude that $\vdash_{\mathcal{H}_{\mathsf{C}}} \langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \bot$. Since $\mathcal{H}_{\mathsf{C}}(*,-\!\!*)$ extends $\mathcal{H}_{\mathsf{C}}$, we

have $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \bot$. By propositional reasoning, $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathrel{-\!\!\circledast} \top$. Otherwise, let us assume that $\langle \mathtt{sep} \rangle(\varphi,\psi)$ is satisfiable.

Structure of the remaining part of the proof. Before presenting the technical arguments for the derivation of $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathrel{-\!\!\circledast} \top$ when $\langle \mathtt{sep} \rangle(\varphi,\psi)$ is satisfiable, let us explain what are the main ingredients. The proof establishing that $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow \varphi \mathrel{-\!\!\circledast} \top$ is by induction on the number j of variables $\mathtt{x} \in \mathtt{X}$ for which $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi$ holds. As φ, ψ and $\langle \mathtt{sep} \rangle(\varphi,\psi)$ are currently assumed to be satisfiable, they have exactly the same equalities and inequalities and this is used in the proof. The base case $j = 0$ can be handled using several derivations taking advantage of Lemma 6.3. For the induction step $j > 0$, some more substantial work is needed and this is briefly described below. We distinguish the case $\max_{\mathtt{size}}(\varphi) < \alpha$ from the case $\max_{\mathtt{size}}(\varphi) = \alpha$. Both cases, we introduce the formula $\mathit{Atom}(\mathtt{x}_i)$ where $\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathsf{Lt}} \varphi$.

$$\mathit{Atom}(\mathtt{x}_i) \stackrel{\text{def}}{=} \begin{cases} \mathtt{x}_i \hookrightarrow \mathtt{y} \wedge \mathtt{size} = 1 & \text{if } \mathtt{x}_i \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi, \text{ for some } \mathtt{y} \in \mathtt{X} \\ \mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \wedge \bigwedge_{\mathtt{y} \in \mathtt{X}} \neg \mathtt{x}_i \hookrightarrow \mathtt{y} & \text{otherwise} \end{cases}$$

In the case $\max_{\mathtt{size}}(\varphi) < \alpha$, we introduce a formula φ' as a very slight variant of φ such that φ' enjoys the following essential properties.

(**A**) φ' is a satisfiable core type in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$.
(**B**) $(\mathit{Atom}(\mathtt{x}_i) * \varphi') \Rightarrow \varphi$ is valid.
(**C**) $(\langle \mathtt{sep} \rangle(\varphi,\psi) * \mathit{Atom}(\mathtt{x}_i)) \Rightarrow \langle \mathtt{sep} \rangle(\varphi',\psi)$ is valid.

In order to conclude $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$, we take advantage of the completeness of $\mathcal{H}_{\mathsf{C}}(*)$ to derive the tautologies in (**B**) and (**C**). Moreover, as by construction of φ', we have $\neg\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathsf{Lt}} \varphi'$ and, for every $\mathtt{y} \in \mathtt{X}$, $\neg\mathtt{alloc}(\mathtt{y}) \subseteq_{\mathsf{Lt}} \varphi$ implies $\neg\mathtt{alloc}(\mathtt{y}) \subseteq_{\mathsf{Lt}} \varphi'$, we shall be able to apply the induction hypothesis on φ' to get $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi',\psi) \Rightarrow (\varphi' \mathrel{-\!\!\circledast} \top)$, which will be essential in the final derivation for $\langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$.

In the remaining case $\max_{\mathtt{size}}(\varphi) = \alpha$, we are still looking for some formula φ' such that $\varphi' * \mathit{Atom}(\mathtt{x}_i) \Rightarrow \varphi$ is valid but we cannot hope for φ' to be a core type in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$. Instead, we introduce two core types φ'_α and $\varphi'_{\alpha-1}$, and define φ' as $\varphi'_\alpha \vee \varphi'_{\alpha-1}$. The only difference between φ'_α and $\varphi'_{\alpha-1}$ rests on the fact that $\mathtt{size} \geqslant \alpha \subseteq_{\mathsf{Lt}} \varphi'_\alpha$ whereas $\neg\mathtt{size} \geqslant \alpha \subseteq_{\mathsf{Lt}} \varphi'_{\alpha-1}$ (both formulae contain $\mathtt{size} \geqslant \alpha - 1$). Similarly to the previous case, the properties below shall be shown.

(**D**) φ'_α and $\varphi'_{\alpha-1}$ are satisfiable core types in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$
(**E**) $(\mathit{Atom}(\mathtt{x}_i) * (\varphi'_\alpha \vee \varphi'_{\alpha-1})) \Rightarrow \varphi$ is valid.
(**F**) $(\langle \mathtt{sep} \rangle(\varphi,\psi) * \mathit{Atom}(\mathtt{x}_i)) \Rightarrow \langle \mathtt{sep} \rangle(\varphi'_\alpha,\psi) \vee \langle \mathtt{sep} \rangle(\varphi'_{\alpha-1},\psi)$ is valid.

The derivation of $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi,\psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$ follows then a principle similar to one for the case $\max_{\mathtt{size}}(\varphi) < \alpha$.

Now, let us present the technical developments. Directly from the definition of $\langle \mathtt{sep} \rangle(\varphi,\psi)$, the following simple facts hold.

1. φ, ψ and $\langle \mathtt{sep} \rangle(\varphi,\psi)$ have exactly the same equalities and inequalities.
2. $\neg\mathtt{size} \geqslant 0$ is not part of $\langle \mathtt{sep} \rangle(\varphi,\psi)$, and therefore, following the definition of $\langle \mathtt{sep} \rangle(\varphi,\psi)$, there are no $\mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi$ and $\neg\mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi$ with $\beta_1 \geqslant \beta_2$.
3. $\mathtt{x} \neq \mathtt{x}$ does not belong to $\langle \mathtt{sep} \rangle(\varphi,\psi)$. In particular, by definition of $\langle \mathtt{sep} \rangle(\varphi,\psi)$, none of the following conditions apply:
   – there is $\mathtt{x} \in \mathtt{X}$ such that $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi$ and $\neg\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \psi$,
   – there are $\mathtt{x}, \mathtt{y} \in \mathtt{X}$ such that $\mathtt{x} \hookrightarrow \mathtt{y} \in \varphi$ and $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi$,

– there are $\mathtt{x}, \mathtt{y} \in \mathtt{X}$ such that $\mathtt{alloc(x)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi$ and $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \psi$.

From (1), we know that $\langle \mathtt{sep} \rangle(\varphi, \psi)$ and φ satisfy the same (in)equalities. Similarly to the proof of Lemma 5.4, let $\mathtt{x}_1, \ldots \mathtt{x}_n$ be a maximal enumeration of representatives of the equivalence classes (one per equivalence class) such that $\mathtt{alloc}(\mathtt{x}_i)$ occurs in φ. As it is maximal, for every $\mathtt{alloc(x)}$ in $\mathtt{Lt}(\varphi)$ there is $i \in [1, n]$ such that $\mathtt{x}_i$ is syntactically equal to $\mathtt{x}$. Moreover, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, for every $i \in [1, n]$, $\neg \mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. The proof of $\vdash_{\mathcal{H}_{\mathsf{C}}(*, -\!\!*)} \langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow \varphi \mathrel{-\!\!\circledast} \top$ is by induction on the number j of variables $\mathtt{x} \in \mathtt{X}$ for which $\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi$ holds.

base case: $j = 0$**:** In the base case, no formula $\mathtt{alloc(x)}$ occurs positively in φ. Since φ is a core type, this implies that for every $\mathtt{x} \in \mathtt{X}$, $\neg \mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi$. Moreover, since φ is satisfiable, for every $\mathtt{x}, \mathtt{y} \in \mathtt{X}$, $\neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi$ (see the axiom $\mathbf{(A_3^C)}$). Therefore, the core type φ is syntactically equivalent (up to associativity and commutativity of conjunction) to the formula $\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \wedge \varphi_{\mathtt{(in)eq}}$, where

- $\varphi_{\mathtt{size}} \stackrel{\text{def}}{=} \bigwedge \big(\{ \mathtt{size} \geqslant \beta \subseteq_{\mathtt{Lt}} \varphi \} \cup \{ \neg \mathtt{size} \geqslant \beta \subseteq_{\mathtt{Lt}} \varphi \} \big)$,
- $\varphi_{\neg \mathtt{alloc}} \stackrel{\text{def}}{=} \bigwedge_{\mathtt{x} \in \mathtt{X}} \neg \mathtt{alloc(x)}$,
- $\varphi_{\not\mapsto} \stackrel{\text{def}}{=} \bigwedge_{\mathtt{x}, \mathtt{y} \in \mathtt{X}} \neg \mathtt{x} \hookrightarrow \mathtt{y}$,
- $\varphi_{\mathtt{(in)eq}} \stackrel{\text{def}}{=} \bigwedge \{ \mathtt{x} \sim \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi \mid \sim \in \{=, \neq\} \}$.

Since φ is satisfiable, so is $\varphi_{\mathtt{size}}$. We show that $\vdash_{\mathcal{H}_{\mathsf{C}}(*, -\!\!*)} (\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto}) \mathrel{-\!\!\circledast} \top$:

1	$\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \mathrel{-\!\!\circledast} \top$	$\mathbf{(I^{-\!\!*}_{6.3.12})}$
2	$\neg \mathtt{alloc(x)} \Rightarrow \neg \mathtt{x} \hookrightarrow \mathtt{y}$	$\mathbf{(A_3^C)}$, PC
3	$\varphi_{\neg \mathtt{alloc}} \Rightarrow \varphi_{\not\mapsto}$	PC, repeated 2
4	$\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \Rightarrow \varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto}$	PC, 3
5	$(\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \mathrel{-\!\!\circledast} \top) \Rightarrow (\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \mathrel{-\!\!\circledast} \top)$	$\mathbf{(I^{-\!\!*}_{6.3.4})}$, 4
6	$\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \mathrel{-\!\!\circledast} \top$	Modus Ponens, 1, 5

Now, let us treat the formula $\varphi_{\mathtt{(in)eq}}$. From the definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, we have $\varphi_{\mathtt{(in)eq}} \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, and so by propositional reasoning, $\vdash_{\mathcal{H}_{\mathsf{C}}(*, -\!\!*)} \langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow \varphi_{\mathtt{(in)eq}}$. This allows us to conclude that

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*, -\!\!*)} \langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow \big((\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \wedge \varphi_{\mathtt{(in)eq}}) \mathrel{-\!\!\circledast} \top \big), \qquad (\dagger)$$

by induction on the number of literals $\mathtt{x} \sim \mathtt{y}$ appearing in $\varphi_{\mathtt{(in)eq}}$, and by relying on the two theorems $\mathbf{(I^{-\!\!*}_{6.3.10})}$ and $\mathbf{(I^{-\!\!*}_{6.3.11})}$. In the base case, $\varphi_{\mathtt{(in)eq}} = \top$, and so

7	$\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \Rightarrow \varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \wedge \varphi_{\mathtt{(in)eq}}$	PC
8	$(\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \mathrel{-\!\!\circledast} \top) \Rightarrow (\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \wedge \varphi_{\mathtt{(in)eq}} \mathrel{-\!\!\circledast} \top)$	$\mathbf{(I^{-\!\!*}_{6.3.4})}$, 7
9	$\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \wedge \varphi_{\mathtt{(in)eq}} \mathrel{-\!\!\circledast} \top$	Modus Ponens, 6, 8
10	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \wedge \varphi_{\mathtt{(in)eq}} \mathrel{-\!\!\circledast} \top)$	PC, 9

In the induction step, let $\varphi_{\mathtt{(in)eq}} = \varphi'_{\mathtt{(in)eq}} \wedge \mathtt{x} \sim \mathtt{y}$, where $\mathtt{x} \sim \mathtt{y} \nsubseteq_{\mathtt{Lt}} \varphi'_{\mathtt{(in)eq}}$. We have,

1	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (\varphi_{\mathtt{size}} \wedge \varphi_{\neg \mathtt{alloc}} \wedge \varphi_{\not\mapsto} \wedge \varphi'_{\mathtt{(in)eq}} \mathrel{-\!\!\circledast} \top)$	Induction Hypothesis

2	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow \mathtt{x} \sim \mathtt{y}$	PC, as $\varphi_{\mathtt{(in)eq}} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$
3	$\mathtt{x} \sim \mathtt{y} \wedge (\varphi_{\mathtt{size}} \wedge \varphi_{\neg\mathtt{alloc}} \wedge \varphi_{\mapsto} \wedge \varphi'_{\mathtt{(in)eq}} \mathrel{-\!\!\circledast} \top) \Rightarrow$ $(\varphi_{\mathtt{size}} \wedge \varphi_{\neg\mathtt{alloc}} \wedge \varphi_{\mapsto} \wedge \varphi'_{\mathtt{(in)eq}} \wedge \mathtt{x} \sim \mathtt{y} \mathrel{-\!\!\circledast} \top)$	$\mathbf{(I^{-\!*}_{6.3.10})/(I^{-\!*}_{6.3.11})}$
4	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (\varphi_{\mathtt{size}} \wedge \varphi_{\neg\mathtt{alloc}} \wedge \varphi_{\mapsto} \wedge \varphi'_{\mathtt{(in)eq}} \wedge \mathtt{x} \sim \mathtt{y} \mathrel{-\!\!\circledast} \top)$	PC, 1, 2, 3
5	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (\varphi_{\mathtt{size}} \wedge \varphi_{\neg\mathtt{alloc}} \wedge \varphi_{\mapsto} \wedge \varphi_{\mathtt{(in)eq}} \mathrel{-\!\!\circledast} \top)$	Def. of $\varphi'_{\mathtt{(in)eq}}$, 4

Since $\varphi_{\mathtt{size}} \wedge \varphi_{\neg\mathtt{alloc}} \wedge \varphi_{\mapsto} \wedge \varphi_{\mathtt{(in)eq}}$ is equivalent to φ, from (†) and by $\mathbf{(I^{-\!*}_{6.3.4})}$, we conclude that $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!*)} \langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow \varphi \mathrel{-\!\!\circledast} \top$.

induction step: $j \geqslant 1$**:** In this case, let $i \in [1, n]$ such that $\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathsf{Lt}} \varphi$ and thus, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, $\neg\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. As announced earlier, we define the formula:

$$Atom(\mathtt{x}_i) \stackrel{\text{def}}{=} \begin{cases} \mathtt{x}_i \hookrightarrow \mathtt{y} \wedge \mathtt{size} = 1 & \text{if } \mathtt{x}_i \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi, \text{ for some } \mathtt{y} \in \mathtt{X} \\ \mathtt{alloc}(\mathtt{x}_i) \wedge \mathtt{size} = 1 \wedge \bigwedge_{\mathtt{y} \in \mathtt{X}} \neg \mathtt{x}_i \hookrightarrow \mathtt{y} & \text{otherwise} \end{cases}$$

Notice that, if there is $\mathtt{y} \in \mathtt{X}$ such that $\mathtt{x}_i \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$, then the axiom schema $\mathbf{(A^{-\!*}_{22})}$ can be instantiated to $\neg\mathtt{alloc}(\mathtt{x}_i) \Rightarrow (Atom(\mathtt{x}_i) \mathrel{-\!\!\circledast} \top)$. Otherwise (for all $\mathtt{y} \in \mathtt{X}$, $\mathtt{x}_i \hookrightarrow \mathtt{y} \not\subseteq_{\mathsf{Lt}} \varphi$) this formula is an instantiation of the axiom schema $\mathbf{(A^{-\!*}_{23})}$. This allows us to show the following theorem:

$$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow \big(Atom(\mathtt{x}_i) \mathrel{-\!\!\circledast} (\langle \mathtt{sep} \rangle(\varphi, \psi) * Atom(\mathtt{x}_i)) \big) \qquad (\ddagger)$$

1	$\neg\mathtt{alloc}(\mathtt{x}_i) \Rightarrow (Atom(\mathtt{x}_i) \mathrel{-\!\!\circledast} \top)$	$\mathbf{(A^{-\!*}_{22})/(A^{-\!*}_{23})}$
2	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow \neg\mathtt{alloc}(\mathtt{x}_i)$	Def. of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, PC
3	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (Atom(\mathtt{x}_i) \mathrel{-\!\!\circledast} \top)$	$\Rightarrow$**-Tr**, 1, 2
4	$\langle \mathtt{sep} \rangle(\varphi, \psi) * Atom(\mathtt{x}_i) \Rightarrow \langle \mathtt{sep} \rangle(\varphi, \psi) * Atom(\mathtt{x}_i)$	PC
5	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (Atom(\mathtt{x}_i) \mathrel{-\!\!*} \langle \mathtt{sep} \rangle(\varphi, \psi) * Atom(\mathtt{x}_i))$	$*$**-Adj**, 4
6	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (Atom(\mathtt{x}_i) \mathrel{-\!\!\circledast} \langle \mathtt{sep} \rangle(\varphi, \psi) * Atom(\mathtt{x}_i))$	$\mathbf{(I^{-\!*}_{6.3.9})}$, 3, 5, PC

From the hypothesis $\mathrm{card}(\mathtt{X}) \leqslant \alpha$, together with $\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathsf{Lt}} \varphi$ and the fact that φ is satisfiable, we have $\max_{\mathtt{size}}(\varphi) \geqslant 1$ (see $\mathbf{(I^{\mathsf{C}}_6)}$, instantiated with $\mathtt{X} = \{\mathtt{x}_i\}$). In order to show that $\vdash_{\mathcal{H}_{\mathsf{C}}*,-\!*} \langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$, we split the proof depending on whether $\max_{\mathtt{size}}(\varphi) < \alpha$ holds.

case: $\max_{\mathtt{size}}(\varphi) < \alpha$**:** Since φ is a satisfiable core type in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, by definition of $\max_{\mathtt{size}}(.)$, we have $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \wedge \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathsf{Lt}} \varphi$. Below, we consider the formula φ' obtained from φ by:

- replacing $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \subseteq_{\mathsf{Lt}} \varphi$ with $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi)$,
- for every $\mathtt{x} \in \mathtt{X}$ such that $\mathtt{x} = \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi$, replacing every literal $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi$ with $\neg\mathtt{alloc}(\mathtt{x})$, and every literal $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$ with $\neg\mathtt{x} \hookrightarrow \mathtt{y}$, where $\mathtt{y} \in \mathtt{X}$.

Explicitly,

$$\begin{aligned}\varphi' \stackrel{\text{def}}{=}\ & \bigwedge\{\mathtt{x} \sim \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi \mid {\sim} \in \{=, \neq\}\} \wedge \bigwedge\{\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi \mid \mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi\} \wedge \\ & \bigwedge\{\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi\} \wedge \bigwedge\{\neg\mathtt{alloc(x)} \mid \mathtt{x} = \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi\} \wedge \bigwedge\{\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi \mid \mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi\} \wedge \\ & \bigwedge\{\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi\} \wedge \bigwedge\{\neg\mathtt{x} \hookrightarrow \mathtt{y} \mid \mathtt{x} = \mathtt{x}_i \wedge \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi\} \wedge \neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \wedge \\ & \bigwedge\{\mathtt{size} \geqslant \beta \subseteq_{\mathsf{Lt}} \varphi \mid \beta < \max_{\mathtt{size}}(\varphi)\} \wedge \bigwedge\{\neg\mathtt{size} \geqslant \beta \subseteq_{\mathsf{Lt}} \varphi\}.\end{aligned}$$

The formula φ' enjoys the following properties (to be shown below):

A. φ' is a satisfiable core type in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$.

B. $(\mathit{Atom}(\mathtt{x}_i) * \varphi') \Rightarrow \varphi$ is valid.

C. $(\langle\mathtt{sep}\rangle(\varphi, \psi) * \mathit{Atom}(\mathtt{x}_i)) \Rightarrow \langle\mathtt{sep}\rangle(\varphi', \psi)$ is valid.

Fundamentally, φ' enjoys the induction hypothesis, which reveals to be useful later on. *Proof of* (**A**). Since φ' is obtained from φ simply by changing the polarity of some of the literals in $\mathsf{Lt}(\varphi)$, clearly φ' is in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$. To show that φ' is satisfiable, we rely on the fact that φ is satisfiable. Let (s, h) be a memory state satisfying φ. Since $\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathsf{Lt}} \varphi$, we conclude that $s(\mathtt{x}_i) \in \mathrm{dom}(h)$. Let us consider the disjoint heaps h_1 and h_2 such that $h = h_1 + h_2$ and $\mathrm{dom}(h_1) = \{s(\mathtt{x}_i)\}$. We show that $(s, h_2) \models \varphi'$ by considering every $L \in \mathsf{Lt}(\varphi')$ and showing that $(s, h_2) \models L$.

case: $L = \mathtt{x} \sim \mathtt{y}$**, where** ${\sim} \in \{=, \neq\}$**:** By definition of φ', $(s, h) \models L$ and therefore $s(\mathtt{x}) \sim s(\mathtt{y})$. Thus, $(s, h_2) \models L$.

case: $L = \neg\mathtt{alloc(x)}$**:** If $\mathtt{x} = \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi$ then $s(\mathtt{x}) \in \mathrm{dom}(h_1)$, and therefore, by $h_1 \sharp h_2$, $s(\mathtt{x}) \notin \mathrm{dom}(h_2)$. So, $(s, h_2) \models \neg\mathtt{alloc(x)}$. Otherwise $(\mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi)$, by definition of φ', we have $\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi$. So $s(\mathtt{x}) \notin \mathrm{dom}(h)$ and, from $h_2 \sqsubseteq h$, we conclude that $(s, h_2) \models \neg\mathtt{alloc(x)}$.

case: $L = \neg\mathtt{x} \hookrightarrow \mathtt{y}$**:** Similar to the previous case. Briefly, if $\mathtt{x} = \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi$ then, by definition of $\mathit{Atom}(\mathtt{x}_i)$, $(s, h_2) \not\models \mathtt{alloc(x)}$, which implies $(s, h_2) \models \neg\mathtt{x} \hookrightarrow \mathtt{y}$. Otherwise, by definition of φ', $\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi$ and thus $(s, h) \models \neg\mathtt{x} \hookrightarrow \mathtt{y}$. From $h_2 \sqsubseteq h$, we conclude that $(s, h_2) \models \neg\mathtt{x} \hookrightarrow \mathtt{y}$.

case: $L = \mathtt{alloc(x)}$**:** By definition of φ', $\mathtt{alloc(x)} \wedge \mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi$. Therefore $s(\mathtt{x}) \in \mathrm{dom}(h)$ and, by definition of $\mathit{Atom}(\mathtt{x}_i)$, $s(\mathtt{x}) \notin \mathrm{dom}(h_1)$. Since $h = h_1 + h_2$, we conclude that $(s, h_2) \models \mathtt{alloc(x)}$.

case: $L = \mathtt{x} \hookrightarrow \mathtt{y}$**:** Similar to the previous case. By definition of φ', we have $\mathtt{x} \hookrightarrow \mathtt{y} \wedge \mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi$. Thus, $h(s(\mathtt{x})) = s(\mathtt{y})$. By definition of $\mathit{Atom}(\mathtt{x}_i)$, $s(\mathtt{x}) \in \mathrm{dom}(h_2)$ and thus $h_2(s(\mathtt{x})) = s(\mathtt{y})$. So, $(s, h_2) \models \mathtt{x} \hookrightarrow \mathtt{y}$.

case: $L = \mathtt{size} \geqslant \beta$**:** By definition of φ', $\beta < \max_{\mathtt{size}}(\varphi)$. Since $(s, h) \models \varphi$, we have $\mathrm{card}(\mathrm{dom}(h)) \geqslant \max_{\mathtt{size}}(\varphi)$. By definition of $\mathit{Atom}(\mathtt{x}_i)$ and from $h = h_1 + h_2$, we have $\mathrm{card}(\mathrm{dom}(h_2)) = \mathrm{card}(\mathrm{dom}(h)) - 1 \geqslant \max_{\mathtt{size}}(\varphi) - 1 \geqslant \beta$. Therefore, $(s, h_2) \models \mathtt{size} \geqslant \beta$.

case: $L = \neg\mathtt{size} \geqslant \beta$**:** By definition of φ', $\neg\mathtt{size} \geqslant \beta \subseteq_{\mathsf{Lt}} \varphi$ or $\beta = \max_{\mathtt{size}}(\varphi)$. In the former case, since φ is satisfiable, we know that $\beta > \max_{\mathtt{size}}(\varphi)$. Therefore, in both cases we have $\beta \geqslant \max_{\mathtt{size}}(\varphi)$. Moreover, as $(s, h) \models \varphi$ and $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathsf{Lt}} \varphi$, we have $\mathrm{card}(\mathrm{dom}(h)) \leqslant \max_{\mathtt{size}}(\varphi)$. Since $\mathrm{card}(\mathrm{dom}(h_1)) = 1$, by $h = h_1 + h_2$ we derive $\mathrm{card}(\mathrm{dom}(h_2)) < \max_{\mathtt{size}}(\varphi) \leqslant \beta$. Therefore, $(s, h_2) \models \neg\mathtt{size} \geqslant \beta$. □

$$\bigwedge \left\{ \mathtt{x} \sim \mathtt{y} \subseteq_{\mathsf{Lt}} \{\varphi' \mid \psi\} \,\middle|\, \sim \in \{=, \neq\} \right\}$$
$$\wedge \bigwedge \{ \neg \mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \psi \}$$
$$\wedge \bigwedge \{ \neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi \}$$
$$\wedge \bigwedge \left\{ \mathtt{x} \neq \mathtt{x} \,\middle|\, \begin{array}{r} \mathtt{alloc}(\mathtt{x}) \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi' \\ \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$
$$\wedge \bigwedge \left\{ \mathtt{x} \neq \mathtt{x} \,\middle|\, \begin{array}{r} \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi' \\ \neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$
$$\wedge \bigwedge \left\{ \mathtt{x} \neq \mathtt{x} \,\middle|\, \begin{array}{r} \mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi' \\ \neg \mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$
$$\wedge \bigwedge \left\{ \mathtt{alloc}(\mathtt{x}) \,\middle|\, \begin{array}{r} \neg \mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi' \\ \mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$
$$\wedge \bigwedge \left\{ \neg \mathtt{alloc}(\mathtt{x}) \,\middle|\, \mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi' \right\}$$
$$\wedge \bigwedge \left\{ \mathtt{x} \hookrightarrow \mathtt{y} \,\middle|\, \begin{array}{r} \neg \mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi' \\ \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$
$$\wedge \bigwedge \left\{ \mathtt{size} \geqslant \beta_2 + 1 \dot{-} \beta_1 \,\middle|\, \begin{array}{r} \neg \mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi' \\ \mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$
$$\wedge \bigwedge \left\{ \neg \mathtt{size} \geqslant \beta_2 \dot{-} \beta_1 \,\middle|\, \begin{array}{r} \mathtt{size} \geqslant \beta_1 \subseteq_{\mathsf{Lt}} \varphi' \\ \neg \mathtt{size} \geqslant \beta_2 \subseteq_{\mathsf{Lt}} \psi \end{array} \right\}$$

Figure 9: The formula $\langle \mathtt{sep} \rangle(\varphi', \psi)$.

Proof of (**B**). Let $(s,h) \models \mathit{Atom}(\mathtt{x}_i) * \varphi'$. So, there are h_1 and h_2 such that $h = h_1 + h_2$, $(s,h_1) \models \mathit{Atom}(\mathtt{x}_i)$ and $(s,h_2) \models \varphi'$. By definition of $\mathit{Atom}(\mathtt{x}_i)$, $\mathrm{dom}(h_1) = \{s(\mathtt{x}_i)\}$. In order to prove (**B**), we show that $(s,h) \models L$, for every literal $L \in \mathsf{Lt}(\varphi)$.

case: $L = \mathtt{x} \sim \mathtt{y}$**, where** $\sim \in \{=, \neq\}$**:** By definition of φ', $(s,h_2) \models L$ and therefore $s(\mathtt{x}) \sim s(\mathtt{y})$. Hence, $(s,h) \models L$.

case: $L = \neg\mathtt{alloc}(\mathtt{x})$**:** By definition of $\mathit{Atom}(\mathtt{x}_i)$, $\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathsf{Lt}} \varphi$ and therefore $s(\mathtt{x}) \notin \mathrm{dom}(h_1)$. By definition of φ', for every $\mathtt{y} \in \mathtt{X}$, $\mathtt{alloc}(\mathtt{y}) \subseteq_{\mathsf{Lt}} \varphi'$ implies $\mathtt{alloc}(\mathtt{y}) \subseteq_{\mathsf{Lt}} \varphi$. Therefore, $s(\mathtt{x}) \notin \mathrm{dom}(h_2)$. We conclude that $s(\mathtt{x}) \notin \mathrm{dom}(h)$, and so $(s,h) \models \neg\mathtt{alloc}(\mathtt{x})$.

case: $L = \neg\mathtt{x} \hookrightarrow \mathtt{y}$**:** Similar to the previous case. Briefly, by definition of $\mathit{Atom}(\mathtt{x}_i)$, $(s,h_1) \models \neg\mathtt{x} \hookrightarrow \mathtt{y}$. By definition of φ', $(s,h_2) \models \neg\mathtt{x} \hookrightarrow \mathtt{y}$. So, $(s,h) \models \neg\mathtt{x} \hookrightarrow \mathtt{y}$.

case: $L = \mathtt{alloc}(\mathtt{x})$**:** If $\mathtt{x} = \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi$, then $s(\mathtt{x}) = s(\mathtt{x}_i)$ (first case of the proof), and by definition of $\mathit{Atom}(\mathtt{x}_i)$, $s(\mathtt{x}) \in \mathrm{dom}(h_1)$. As $h_1 \sqsubseteq h$, we conclude that $(s,h) \models \mathtt{alloc}(\mathtt{x})$. Otherwise, if $\mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi$, then by definition of φ' we have $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathsf{Lt}} \varphi'$. This implies that $s(\mathtt{x}) \in \mathrm{dom}(h_2)$ and so, from $h_2 \sqsubseteq h$, we conclude that $(s,h) \models \mathtt{alloc}(\mathtt{x})$.

case: $L = \mathtt{x} \hookrightarrow \mathtt{y}$**:** Similar to the previous case. Briefly, if $\mathtt{x} = \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi$ then, by definition of $\mathit{Atom}(\mathtt{x}_i)$, $(s,h_1) \models \mathtt{x} \hookrightarrow \mathtt{y}$ and so $(s,h) \models \mathtt{x} \hookrightarrow \mathtt{y}$. Otherwise $(\mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi)$, $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi'$ and therefore $(s,h_2) \models \mathtt{x} \hookrightarrow \mathtt{y}$. So, $(s,h) \models \mathtt{x} \hookrightarrow \mathtt{y}$.

case: $L = \mathtt{size} \geqslant \beta$**:** If $\beta < \max_{\mathtt{size}}(\varphi)$, then directly by definition of φ', we have $(s,h_2) \models \mathtt{size} \geqslant \beta$. From $h_2 \sqsubseteq h$, we conclude that $(s,h) \models \mathtt{size} \geqslant \beta$. Otherwise, $\beta = \max_{\mathtt{size}}(\varphi)$. Recall that $\max_{\mathtt{size}}(\varphi) \geqslant 1$ and so, by definition of φ', $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) - 1 \subseteq_{\mathsf{Lt}} \varphi'$. Thus, $\mathrm{card}(\mathrm{dom}(h_2)) \geqslant \max_{\mathtt{size}}(\varphi) - 1$. By definition of $\mathit{Atom}(\mathtt{x}_i)$ we have $\mathrm{card}(\mathrm{dom}(h_1)) = 1$. As $h = h_1 + h_2$, we conclude that $(s,h) \models \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi)$.

case: $L = \neg\mathtt{size} \geqslant \beta$**:** As φ is satisfiable, $\beta > \max_{\mathtt{size}}(\varphi)$. By definition of the formula φ', $\neg\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) \subseteq_{\mathsf{Lt}} \varphi'$ and thus $\mathrm{card}(\mathrm{dom}(h_2)) < \max_{\mathtt{size}}(\varphi)$. From $\mathrm{card}(\mathrm{dom}(h_1)) = 1$ we derive $\mathrm{card}(\mathrm{dom}(h)) \leqslant \max_{\mathtt{size}}(\varphi) < \beta$, which allows us to conclude that $(s,h) \models \neg\mathtt{size} \geqslant \beta$. □

*Proof of (**C**).* Figure 9 recalls the definition of $\langle \mathtt{sep} \rangle(\varphi', \psi)$. First of all, notice that it cannot be that there is $\mathtt{x} \in \mathtt{X}$ such that $\mathtt{x} \neq \mathtt{x} \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi', \psi)$. Indeed, *ad*

absurdum, suppose the opposite. By definition of $\langle \mathtt{sep} \rangle(\varphi', \psi)$, this implies that (1) $\mathtt{alloc(x)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi'$ and $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \psi$, (2) $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi'$ and $\neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \psi$, or (3) $\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi'$ and $\neg \mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \psi$. By definition of φ', this implies that (1) $\mathtt{alloc(x)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi$, (2) $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi$ or (3) $\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi$. However, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, this implies that $\mathtt{x} \neq \mathtt{x} \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, in contradiction with the satisfiability of $\langle \mathtt{sep} \rangle(\varphi, \psi)$. Therefore, below we assume that for all $\mathtt{x} \in \mathtt{X}$, $\mathtt{x} \neq \mathtt{x} \not\subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi', \psi)$.

Let $(s, h) \models \langle \mathtt{sep} \rangle(\varphi, \psi) * \mathit{Atom}(\mathtt{x}_i)$. There are h_1 and h_2 such that $h = h_1 + h_2$, $(s, h_1) \models \langle \mathtt{sep} \rangle(\varphi, \psi)$ and $(s, h_2) \models \mathit{Atom}(\mathtt{x}_i)$. By definition of $\mathit{Atom}(\mathtt{x}_i)$, $\mathrm{dom}(h_2) = \{s(\mathtt{x}_i)\}$. To prove (**C**), we show that $(s, h) \models L$, for every literal $L \in \mathtt{Lt}(\langle \mathtt{sep} \rangle(\varphi', \psi))$.

case: $L = \mathtt{x} \sim \mathtt{y}$**, where** $\sim \in \{=, \neq\}$**:** By definition of $\langle \mathtt{sep} \rangle(\varphi', \psi)$, $L \subseteq_{\mathtt{Lt}} \{\varphi' \mid \psi\}$ and so, by definition of φ', $L \subseteq_{\mathtt{Lt}} \{\varphi \mid \psi\}$. By definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, $L \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. From $(s, h_1) \models \langle \mathtt{sep} \rangle(\varphi, \psi)$ we derive $s(\mathtt{x}) \sim s(\mathtt{y})$. So, $(s, h) \models L$.

case: $L = \neg \mathtt{alloc(x)}$**:** By definition of $\langle \mathtt{sep} \rangle(\varphi', \psi)$, either $\neg \mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \psi$ or $\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi'$. In the first case, by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, $\neg \mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, and therefore $s(\mathtt{x}) \notin \mathrm{dom}(h_1)$. Moreover, since $\langle \mathtt{sep} \rangle(\varphi, \psi)$ is satisfiable, $\mathtt{alloc(x)} \not\subseteq_{\mathtt{Lt}} \varphi$ (otherwise we would have $\mathtt{x} \neq \mathtt{x} \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$). Therefore, by definition of $\mathit{Atom}(\mathtt{x}_i)$, we conclude that $s(\mathtt{x}) \notin \mathrm{dom}(h_2)$. From $h = h_1 + h_2$, we derive $s(\mathtt{x}) \notin \mathrm{dom}(h)$, and thus $(s, h) \models \neg \mathtt{alloc(x)}$.
In the second case, ($\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi'$), by definition of φ' we have $\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi$ and $\mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathtt{Lt}} \varphi$. By definition of $\mathit{Atom}(\mathtt{x}_i)$, $s(\mathtt{x}) \notin \mathrm{dom}(h_2)$. By definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, $\neg \mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, and therefore $s(\mathtt{x}) \notin \mathrm{dom}(h_1)$. Again, by $h = h_1 + h_2$, we have $(s, h) \models \neg \mathtt{alloc(x)}$.

case: $L = \neg \mathtt{x} \hookrightarrow \mathtt{y}$**:** Following the definition of $\langle \mathtt{sep} \rangle(\varphi', \psi)$, $\neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \psi$ and therefore $\neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. Therefore, $(s, h_1) \models \neg \mathtt{x} \hookrightarrow \mathtt{y}$. Since $\langle \mathtt{sep} \rangle(\varphi, \psi)$ is satisfiable, $\neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi$. By definition of $\mathit{Atom}(\mathtt{x}_i)$, we derive $(s, h_2) \models \neg \mathtt{x} \hookrightarrow \mathtt{y}$. From $h = h_1 + h_2$, $(s, h) \models \neg \mathtt{x} \hookrightarrow \mathtt{y}$.

case: $L = \mathtt{alloc(x)}$**:** By definition of $\langle \mathtt{sep} \rangle(\varphi', \psi)$, we have $\neg \mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi'$ and $\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \psi$. First, let us suppose $\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi$. By definition of φ', $\mathtt{x} = \mathtt{x}_i \subseteq_{\mathtt{Lt}} \varphi$ and so, by definition of $\mathit{Atom}(\mathtt{x}_i)$, $s(\mathtt{x}) \in \mathrm{dom}(h_2)$. From $h_2 \sqsubseteq h$, $(s, h) \models \mathtt{alloc(x)}$. Otherwise ($\neg \mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi$), by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, $\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. So, $s(\mathtt{x}) \in \mathrm{dom}(h_1)$, and by $h_1 \sqsubseteq h$, $(s, h) \models \mathtt{alloc(x)}$.

case: $L = \mathtt{x} \hookrightarrow \mathtt{y}$**:** Similar to the previous case. By definition of $\langle \mathtt{sep} \rangle(\varphi', \psi)$, $\neg \mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi'$ and $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \psi$. First, let us assume $\mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi$. By definition of φ', $\mathtt{x} = \mathtt{x}_i \subseteq_{\mathtt{Lt}} \varphi$. By definition of $\mathit{Atom}(\mathtt{x}_i)$, $s(\mathtt{x}) \in \mathrm{dom}(h_2)$. *Ad absurdum*, suppose $h(s(\mathtt{x})) \neq s(\mathtt{y})$. By definition of $\mathit{Atom}(\mathtt{x}_i)$, we have that $\mathtt{alloc(x)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi$. However, from $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \psi$, this implies $\mathtt{x} \neq \mathtt{x} \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, which contradicts the satisfiability of $\langle \mathtt{sep} \rangle(\varphi, \psi)$. Therefore, $h(s(\mathtt{x})) = s(\mathtt{y})$ and, from $h_2 \sqsubseteq h$, we conclude that $(s, h) \models \mathtt{x} \hookrightarrow \mathtt{y}$. Otherwise ($\neg \mathtt{alloc(x)} \subseteq_{\mathtt{Lt}} \varphi$), by definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$, $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. So, $h_1(s(\mathtt{x})) = s(\mathtt{y})$, and by $h_1 \sqsubseteq h$, we derive $(s, h) \models \mathtt{x} \hookrightarrow \mathtt{y}$.

case: $L = \mathtt{size} \geqslant \beta_2 + 1 \dot{-} \beta_1$**, where** $\neg \mathtt{size} \geqslant \beta_1 \subseteq_{\mathtt{Lt}} \varphi'$ **and** $\mathtt{size} \geqslant \beta_2 \subseteq_{\mathtt{Lt}} \psi$**:** By definition of φ', $\neg \mathtt{size} \geqslant \beta_1 \subseteq_{\mathtt{Lt}} \varphi$, and so $\beta_1 > \max_{\mathtt{size}}(\varphi)$, since φ is satisfiable. By definition of $\langle \mathtt{sep} \rangle(\varphi, \psi)$ and as $\neg \mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi) + 1 \subseteq_{\mathtt{Lt}} \varphi$, we have $\mathtt{size} \geqslant \beta_2 + 1 \dot{-} (\max_{\mathtt{size}}(\varphi) + 1) \subseteq_{\mathtt{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$, which in turn implies $\mathrm{card}(\mathrm{dom}(h_1)) \geqslant \beta_2 \dot{-} \max_{\mathtt{size}}(\varphi)$. By definition of $\mathit{Atom}(\mathtt{x}_i)$,

$\mathrm{card}(\mathrm{dom}(h_2)) \geqslant 1$. By $h = h_1{+}h_2$, $\mathrm{card}(\mathrm{dom}(h)) \geqslant (\beta_2 \dot{-} \max_{\mathtt{size}}(\varphi)) + 1 \geqslant (\beta_2 + 1) \dot{-} \max_{\mathtt{size}}(\varphi)$. As $\beta_1 > \max_{\mathtt{size}}(\varphi)$, $(s,h) \models \mathtt{size} \geqslant \beta_2{+}1 \dot{-} \beta_1$.

case: $L = \neg\mathtt{size} \geqslant \beta_2 \dot{-} \beta_1$**, where** $\mathtt{size} \geqslant \beta_1 \subseteq_{\mathtt{Lt}} \varphi'$ **and** $\neg\mathtt{size} \geqslant \beta_2 \subseteq_{\mathtt{Lt}} \psi$**:** By definition of φ', $\beta_1 < \max_{\mathtt{size}}(\varphi)$. By definition of $\langle\mathtt{sep}\rangle(\varphi,\psi)$, we have $\neg\mathtt{size} \geqslant \beta_2 \dot{-} \max_{\mathtt{size}}(\varphi) \subseteq_{\mathtt{Lt}} \langle\mathtt{sep}\rangle(\varphi,\psi)$. Notice that, since $\langle\mathtt{sep}\rangle(\varphi,\psi)$ is satisfiable, $\beta_2 > \max_{\mathtt{size}}(\varphi)$. Thus, $\mathrm{card}(\mathrm{dom}(h_1)) < \beta_2 - \max_{\mathtt{size}}(\varphi)$. By definition of $\mathit{Atom}(\mathtt{x}_i)$, $\mathrm{card}(\mathrm{dom}(h_2)) \leqslant 1$. From $h = h_1{+}h_2$, we conclude that $\mathrm{card}(\mathrm{dom}(h)) < (\beta_2 - \max_{\mathtt{size}}(\varphi)) + 1$. As $\beta_1 < \max_{\mathtt{size}}(\varphi)$, we have $\beta_2 - \max_{\mathtt{size}}(\varphi) + 1 \leqslant \beta_2 \dot{-} \beta_1$. Therefore, $(s,h) \models \neg\mathtt{size} \geqslant \beta_2 \dot{-} \beta_1$.

Continuing with the proof of Lemma 6.2, we prove $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle\mathtt{sep}\rangle(\varphi,\psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$. Notice that, by the completeness of $\mathcal{H}_{\mathsf{C}}(*)$ (Theorem 5.6), we conclude that the tautologies in (**B**) and (**C**) are derivable in $\mathcal{H}_{\mathsf{C}}(*,-\!\!*)$. Moreover, notice that $\neg\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathtt{Lt}} \varphi'$ and, for every $\mathtt{y} \in \mathtt{X}$, $\neg\mathtt{alloc}(\mathtt{y}) \subseteq_{\mathtt{Lt}} \varphi$ implies $\neg\mathtt{alloc}(\mathtt{y}) \subseteq_{\mathtt{Lt}} \varphi'$. This allows us to rely on the induction hypothesis, and conclude that $\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle\mathtt{sep}\rangle(\varphi',\psi) \Rightarrow (\varphi' \mathrel{-\!\!\circledast} \top)$. The derivation of $\langle\mathtt{sep}\rangle(\varphi,\psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$ is given below:

1	$\langle\mathtt{sep}\rangle(\varphi',\psi) \Rightarrow (\varphi' \mathrel{-\!\!\circledast} \top)$	Induction hypothesis
2	$\mathit{Atom}(\mathtt{x}_i) * \varphi' \Rightarrow \varphi$	(**B**), Theorem 5.6
3	$\langle\mathtt{sep}\rangle(\varphi,\psi) * \mathit{Atom}(\mathtt{x}_i) \Rightarrow \langle\mathtt{sep}\rangle(\varphi',\psi)$	(**C**), Theorem 5.6
4	$(\langle\mathtt{sep}\rangle(\varphi,\psi) * \mathit{Atom}(\mathtt{x}_i)) \Rightarrow (\varphi' \mathrel{-\!\!\circledast} \top)$	$\Rightarrow$**-Tr**, 1, 3
5	$\langle\mathtt{sep}\rangle(\varphi,\psi) \Rightarrow (\mathit{Atom}(\mathtt{x}_i) \mathrel{-\!\!\circledast} \langle\mathtt{sep}\rangle(\varphi,\psi) * \mathit{Atom}(\mathtt{x}_i))$	(‡)
6	$(\mathit{Atom}(\mathtt{x}_i) \mathrel{-\!\!\circledast} \langle\mathtt{sep}\rangle(\varphi,\psi) * \mathit{Atom}(\mathtt{x}_i)) \Rightarrow \big(\mathit{Atom}(\mathtt{x}_i) \mathrel{-\!\!\circledast} (\varphi' \mathrel{-\!\!\circledast} \top)\big)$	$(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.5}})$, 4
7	$\big(\mathit{Atom}(\mathtt{x}_i) \mathrel{-\!\!\circledast} (\varphi' \mathrel{-\!\!\circledast} \top)\big) \Rightarrow (\mathit{Atom}(\mathtt{x}_i) * \varphi' \mathrel{-\!\!\circledast} \top)$	$(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.6}})$
8	$(\mathit{Atom}(\mathtt{x}_i) * \varphi' \mathrel{-\!\!\circledast} \top) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$	$(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.4}})$, 2
9	$\langle\mathtt{sep}\rangle(\varphi,\psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$	$\Rightarrow$**-Tr**, 5, 6, 7, 8

case: $\max_{\mathtt{size}}(\varphi) = \alpha$**:** In this case, we have $\mathtt{size} \geqslant \alpha \subseteq_{\mathtt{Lt}} \varphi$, where we recall that $\alpha = \max_{\mathtt{size}}(\varphi) \geqslant 1$. Following the developments of the previous case, we would like to define a formula φ' for which the formula $\varphi' * \mathit{Atom}(\mathtt{x}_i) \Rightarrow \varphi$ is valid. However, since φ is in $\mathsf{CoreTypes}(\mathtt{X},\alpha)$, we cannot hope for φ' to be a core type in $\mathsf{CoreTypes}(\mathtt{X},\alpha)$. Indeed, because of $\mathtt{size} \geqslant \alpha \subseteq_{\mathtt{Lt}} \varphi$, in order to achieve the valid formula above we must differentiate between the case where φ is satisfied by a memory state (s,h) such that $\mathrm{card}(\mathrm{dom}(h)) > \alpha$, to the case where $\mathrm{card}(\mathrm{dom}(h)) = \alpha$. Therefore, below we introduce two core types φ'_α and $\varphi'_{\alpha-1}$, and define φ' as $\varphi'_\alpha \vee \varphi'_{\alpha-1}$. Since the separating conjunction distributes over disjunctions, after defining these two core types, we can easily adapt the arguments of the previous case to prove that $\langle\mathtt{sep}\rangle(\varphi,\psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$. The formula φ'_α is obtained from φ by replacing, for every $\mathtt{x} \in \mathtt{X}$ such that $\mathtt{x} = \mathtt{x}_i \subseteq_{\mathtt{Lt}} \varphi$, every literal $\mathtt{alloc}(\mathtt{x}) \subseteq_{\mathtt{Lt}} \varphi$ with $\neg\mathtt{alloc}(\mathtt{x})$, and every $\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathtt{Lt}} \varphi$ with $\neg\mathtt{x} \hookrightarrow \mathtt{y}$, where $\mathtt{y} \in \mathtt{X}$. Notice that φ'_α is defined similarly to φ' (in the previous case of the proof), with the exception that we do not modify the polarity of size literals. Explicitly,

φ'_α is defined as follows.

$$\varphi'_\alpha \stackrel{\text{def}}{=} \bigwedge\{\mathtt{x} \sim \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi \mid \sim \in \{=, \neq\}\} \wedge \bigwedge\{\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi \mid \mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi\} \wedge \bigwedge\{\neg\mathtt{alloc(x)} \subseteq_{\mathsf{Lt}} \varphi\} \wedge$$
$$\bigwedge\{\neg\mathtt{alloc(x)} \mid \mathtt{x} = \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi\} \wedge \bigwedge\{\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi \mid \mathtt{x} \neq \mathtt{x}_i \subseteq_{\mathsf{Lt}} \varphi\} \wedge \bigwedge\{\neg\mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi\} \wedge$$
$$\bigwedge\{\neg\mathtt{x} \hookrightarrow \mathtt{y} \mid \mathtt{x} = \mathtt{x}_i \wedge \mathtt{x} \hookrightarrow \mathtt{y} \subseteq_{\mathsf{Lt}} \varphi\} \wedge \bigwedge\{\mathtt{size} \geqslant \beta \mid \beta \in [0, \alpha - 1]\} \wedge \underline{\mathtt{size} \geqslant \alpha}.$$

The formula $\varphi'_{\alpha-1}$ is obtained from φ'_α by replacing $\mathtt{size} \geqslant \alpha$ (highlighted in the definition of φ'_α above), by $\neg\mathtt{size} \geqslant \alpha$. The following properties are satisfied:

D. φ'_α and $\varphi'_{\alpha-1}$ are satisfiable core types in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$,

E. $(\mathit{Atom}(\mathtt{x}_i) * (\varphi'_\alpha \vee \varphi'_{\alpha-1})) \Rightarrow \varphi$ is valid.

F. $(\langle\mathtt{sep}\rangle(\varphi, \psi) * \mathit{Atom}(\mathtt{x}_i)) \Rightarrow \langle\mathtt{sep}\rangle(\varphi'_\alpha, \psi) \vee \langle\mathtt{sep}\rangle(\varphi'_{\alpha-1}, \psi)$ is valid.

Proof of (**D**). The proof is very similar to the one of the property (**A**). Here, we pinpoint the main differences. First of all, since both φ'_α and $\varphi'_{\alpha-1}$ are obtained from φ by changing the polarity of some of the literals in $\mathsf{Lt}(\varphi)$, they are both in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$. To show that φ'_α and $\varphi'_{\alpha-1}$ are satisfiable, we rely on the fact that φ is satisfiable. Let (s, h) be a memory state satisfying φ. Since $\mathtt{size} \geqslant \alpha \subseteq_{\mathsf{Lt}} \varphi$, $\mathrm{card}(\mathrm{dom}(h)) \geqslant \alpha$. Without loss of generality, we can assume $\mathrm{card}(\mathrm{dom}(h)) > \alpha$. Indeed, if $\mathrm{card}(\mathrm{dom}(h)) = \alpha$ it is sufficient to add a memory cell (ℓ, ℓ) to h, such that ℓ does not correspond to a program variable $\mathtt{x} \in \mathtt{X}$. It is straightforward to check that the resulting memory state still satisfies φ. We introduce a second heap h'. Let $\mathtt{L} = \mathrm{dom}(h) \cap \{s(\mathtt{x}) \mid \mathtt{x} \in \mathtt{X}\}$ be the set of locations in $\mathrm{dom}(h)$ that corresponds to variables in $\mathtt{X}$. Since $\mathrm{card}(\mathtt{X}) \leqslant \alpha$, $\mathrm{card}(\mathtt{L}) \leqslant \alpha$. Let $h' \sqsubseteq h$ such that $\mathtt{L} \subseteq \mathrm{dom}(h')$ and $\mathrm{card}(\mathrm{dom}(h')) = \alpha$. Again, it is straightforward to see that (s, h') satisfies φ. Intuitively, we rely on (s, h) to show that φ'_α is satisfiable, and on (s, h') to show that $\varphi'_{\alpha-1}$ is satisfiable. As $\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathsf{Lt}} \varphi$, we have $s(\mathtt{x}) \in \mathrm{dom}(h)$ and $s(\mathtt{x}) \in \mathrm{dom}(h')$. We consider heaps h_1 and h_2 such that $h = h_1 + h_2$ and $\mathrm{dom}(h_1) = \{s(\mathtt{x}_i)\}$. Similarly, we consider heaps h'_1 and h'_2 such that $h' = h'_1 + h'_2$ and $\mathrm{dom}(h'_1) = \{s(\mathtt{x}_i)\}$. We show that $(s, h_2) \models \varphi'_\alpha$ and $(s, h'_2) \models \varphi'_{\alpha-1}$. Let us first discuss the former result. Let $L \in \mathsf{Lt}(\varphi'_\alpha)$. If L is not of the form $\mathtt{size} \geqslant \beta$ or $\neg\mathtt{size} \geqslant \beta$, then $(s, h_2) \models L$ follows exactly as in the proof of (**A**). Otherwise,

case: $L = \mathtt{size} \geqslant \beta$**:** By definition of h_2, $\mathrm{card}(\mathrm{dom}(h_2)) = \mathrm{card}(\mathrm{dom}(h)) - 1 \geqslant \alpha$. Since $\beta \leqslant \alpha$ (as φ'_α is in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$), we conclude that $(s, h_2) \models \mathtt{size} \geqslant \beta$.

case: $L = \neg\mathtt{size} \geqslant \beta$**:** By definition of φ'_α, no literals of the form $\neg\mathtt{size} \geqslant \beta$ belongs to $\mathsf{Lt}(\varphi'_\alpha)$. Therefore, this case does not occur.

This concludes the proof of $(s, h_2) \models \varphi'_\alpha$. For the proof of $(s, h'_2) \models \varphi'_{\alpha-1}$, let us consider $L \in \mathsf{Lt}(\varphi'_{\alpha-1})$. Again, if L is not of the form $\mathtt{size} \geqslant \beta$ or $\neg\mathtt{size} \geqslant \alpha$, then $(s, h'_2) \models L$ follows exactly as in the proof of (**A**) (replacing h by h' and h_2 by h'_2). Otherwise,

case: $L = \mathtt{size} \geqslant \beta$**:** By definition of $\varphi'_{\alpha-1}$, we have $\beta < \alpha$. By definition of h'_2, $\mathrm{card}(\mathrm{dom}(h'_2)) = \mathrm{card}(\mathrm{dom}(h')) - 1 = \alpha - 1$. Therefore, $(s, h'_2) \models \mathtt{size} \geqslant \beta$.

case: $L = \neg\mathtt{size} \geqslant \beta$**:** By definition of $\varphi'_{\alpha-1}$, $\beta = \alpha$. Since $\mathrm{card}(\mathrm{dom}(h'_2)) = \alpha - 1$, we conclude that $(s, h'_2) \models \neg\mathtt{size} \geqslant \beta$. □

Proof of (**E**). The proof is very similar to the one of the property (**B**). We show that $(\mathit{Atom}(\mathtt{x}_i) * \varphi'_\alpha) \Rightarrow \varphi$ and $(\mathit{Atom}(\mathtt{x}_i) * \varphi'_{\alpha-1}) \Rightarrow \varphi$. Then, (**E**) follows as the separating conjunction distributes over disjunction. First, let us consider $(\mathit{Atom}(\mathtt{x}_i) * \varphi'_\alpha) \Rightarrow \varphi$, and a memory state (s, h) satisfying $\mathit{Atom}(\mathtt{x}_i) * \varphi'_\alpha$. There are h_1 and h_2 such that

$h = h_1{+}h_2$, $(s, h_1) \models \mathit{Atom}(\mathtt{x}_i)$ and $(s, h_2) \models \varphi'_\alpha$. Let $L \in \mathsf{Lt}(\varphi)$. Notice that φ does not contain negated $\mathtt{size} \geqslant \beta$ literals. If L is not $\mathtt{size} \geqslant \beta$, for some $\beta \in [0, \alpha]$, then $(s, h) \models L$ follows exactly as it is shown in the proof of (**B**). Otherwise, suppose $L = \mathtt{size} \geqslant \beta$, where $\beta \in [0, \alpha]$. By definition of φ'_α, $\mathtt{size} \geqslant \alpha \subseteq_{\mathsf{Lt}} \varphi'_\alpha$. Hence, $\mathrm{card}(\mathrm{dom}(h_2)) \geqslant \alpha$ and, from $h_2 \sqsubseteq h$, we derive $(s, h) \models \mathtt{size} \geqslant \beta$. So, $(s, h) \models \varphi$.
Let us now consider $(\mathit{Atom}(\mathtt{x}_i) * \varphi'_{\alpha-1}) \Rightarrow \varphi$ and a memory state (s, h) satisfying $\mathit{Atom}(\mathtt{x}_i) * \varphi'_{\alpha-1}$. There are h_1 and h_2 such that $h = h_1{+}h_2$, $(s, h_1) \models \mathit{Atom}(\mathtt{x}_i)$ and $(s, h_2) \models \varphi'_{\alpha-1}$. Let $L \in \mathsf{Lt}(\varphi)$. Again, φ does not contain negated $\mathtt{size} \geqslant \beta$ literals, and if L is not $\mathtt{size} \geqslant \beta$, for some $\beta \in [0, \alpha]$, then $(s, h) \models L$ follows exactly as is shown in the proof of (**B**). Otherwise, suppose $L = \mathtt{size} \geqslant \beta$, where $\beta \in [0, \alpha]$. By definition of $\varphi'_{\alpha-1}$, $\mathtt{size} \geqslant \alpha \dot{-} 1 \subseteq_{\mathsf{Lt}} \varphi'_{\alpha-1}$. Therefore, $\mathrm{card}(\mathrm{dom}(h_2)) \geqslant \alpha - 1$. By definition of $\mathit{Atom}(\mathtt{x}_i)$, $\mathrm{card}(\mathrm{dom}(h_1)) = 1$. From $h = h_1{+}h_2$, we conclude that $\mathrm{card}(\mathrm{dom}(h)) \geqslant \alpha$ and thus $(s, h) \models \mathtt{size} \geqslant \beta$. Therefore, $(s, h) \models \varphi$. □

Proof of (**F**). Recall that $\langle \mathtt{sep} \rangle(\varphi, \psi)$ is satisfiable. In particular, from its definition together with $\mathtt{size} \geqslant \alpha \subseteq_{\mathsf{Lt}} \varphi$, this implies that $\mathtt{size} \geqslant \alpha \subseteq_{\mathsf{Lt}} \psi$, as otherwise we would have $\neg\mathtt{size} \geqslant 0 \subseteq_{\mathsf{Lt}} \langle \mathtt{sep} \rangle(\varphi, \psi)$. So, as ψ is a satisfiable core type in $\mathsf{CoreTypes}(\mathtt{X}, \alpha)$, for all $\beta \in [0, \alpha]$, $\mathtt{size} \geqslant \beta \subseteq_{\mathsf{Lt}} \psi$. Alternatively, ψ does not contain $\neg\mathtt{size} \geqslant \beta$ literals. We look at the definitions of $\langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi)$ and $\langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi)$.

a. Since for all $\beta \in [0, \alpha]$, $\mathtt{size} \geqslant \beta \subseteq_{\mathsf{Lt}} \varphi'_\alpha$ and $\mathtt{size} \geqslant \beta \subseteq_{\mathsf{Lt}} \psi$, we derive that $\langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi)$ does not contain $\mathtt{size} \geqslant \beta$ nor $\neg\mathtt{size} \geqslant \beta$ literals (for all $\beta \in [0, \alpha]$). This holds directly by definition of $\langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi)$, which can be retrieved by substituting φ' by φ'_α in Figure 9.
b. Analogously, we know that $\neg\mathtt{size} \geqslant \alpha \subseteq_{\mathsf{Lt}} \varphi'_{\alpha-1}$ whereas for every $\beta \in [0, \alpha - 1]$, $\mathtt{size} \geqslant \beta \subseteq_{\mathsf{Lt}} \varphi'_{\alpha-1}$, and therefore among all the literals $\mathtt{size} \geqslant \beta$ or $\neg\mathtt{size} \geqslant \beta$ ($\beta \in [0, \alpha]$), $\langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi)$ only contains $\mathtt{size} \geqslant 1$ (occurring positively).

By definition and with the sole exception of the polarity of the formula $\mathtt{size} \geqslant \alpha$ (occurring positively in φ'_α and negatively in $\varphi'_{\alpha-1}$), the two core types $\varphi'_{\alpha-1}$ and φ'_α are equal. Directly by definition of $\langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi)$ and $\langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi)$, together with (a) and (b), this implies that $\langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi)$ is syntactically equal to $\langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi) \wedge \mathtt{size} \geqslant 1$ (up to commutativity and associativity of conjunction). This means that the formula $\langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi) \Rightarrow \langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi)$ is valid, and suggests us that, in order to show (**F**), we can simply establish that $(\langle \mathtt{sep} \rangle(\varphi, \psi) * \mathit{Atom}(\mathtt{x}_i)) \Rightarrow \langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi)$ is valid. As we already stated, φ'_α is defined as φ' (in the previous step of the proof), with the exception that we do not modify the polarity of $\mathtt{size} \geqslant \beta$ literals. Because of this, we can rely on the proof of (**C**). Briefly, we consider a memory state (s, h) satisfying $\langle \mathtt{sep} \rangle(\varphi, \psi) * \mathit{Atom}(\mathtt{x}_i)$. There are h_1 and h_2 such that $h = h_1{+}h_2$, $(s, h_1) \models \langle \mathtt{sep} \rangle(\varphi, \psi)$ and $(s, h_2) \models \mathit{Atom}(\mathtt{x}_i)$. Let $L \in \mathsf{Lt}(\langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi))$. By (a), L is neither of the form $\mathtt{size} \geqslant \beta$ nor of the form $\neg\mathtt{size} \geqslant \beta$. Therefore, $(s, h) \models L$ follows exactly as shown in the proof of (**C**). □

We are now ready to prove that $\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$. By Theorem 5.6, the tautologies in (**D**) and (**F**) are derivable in $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$. Moreover, since $\neg\mathtt{alloc}(\mathtt{x}_i) \subseteq_{\mathsf{Lt}} \{\varphi'_\alpha ; \varphi'_{\alpha-1}\}$ and, for every $\mathtt{y} \in \mathtt{X}$, $\neg\mathtt{alloc}(\mathtt{y}) \subseteq_{\mathsf{Lt}} \varphi$ implies $\neg\mathtt{alloc}(\mathtt{y}) \subseteq_{\mathsf{Lt}} \{\varphi'_\alpha ; \varphi'_{\alpha-1}\}$, we rely on the induction hypothesis to derive

$$\vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi) \Rightarrow (\varphi'_\alpha \mathrel{-\!\!\circledast} \top), \qquad \vdash_{\mathcal{H}_{\mathsf{C}}(*,-\!\!*)} \langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi) \Rightarrow (\varphi'_{\alpha-1} \mathrel{-\!\!\circledast} \top).$$

We derive $\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \top)$ (see Figure 10) concluding the proof of Lemma 6.2 □

1	$\langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi) \Rightarrow (\varphi'_\alpha \mathbin{-\!\!\circledast} \top)$	Induction hypothesis
2	$\langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi) \Rightarrow (\varphi'_{\alpha-1} \mathbin{-\!\!\circledast} \top)$	Induction hypothesis
3	$\mathit{Atom}(\mathtt{x}_i) * (\varphi'_\alpha \vee \varphi'_{\alpha-1}) \Rightarrow \varphi$	(**E**), Theorem 5.6
4	$\langle \mathtt{sep} \rangle(\varphi, \psi) * \mathit{Atom}(\mathtt{x}_i) \Rightarrow \langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi) \vee \langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi)$	(**F**), Theorem 5.6
5	$\langle \mathtt{sep} \rangle(\varphi'_\alpha, \psi) \vee \langle \mathtt{sep} \rangle(\varphi'_{\alpha-1}, \psi) \Rightarrow (\varphi'_\alpha \mathbin{-\!\!\circledast} \top) \vee (\varphi'_{\alpha-1} \mathbin{-\!\!\circledast} \top)$	PC, 1, 2
6	$(\varphi'_\alpha \mathbin{-\!\!\circledast} \top) \vee (\varphi'_{\alpha-1} \mathbin{-\!\!\circledast} \top) \Rightarrow (\varphi'_\alpha \vee \varphi'_{\alpha-1} \mathbin{-\!\!\circledast} \top)$	$\mathbf{(I^{-\!\!*}_{6.3.7})}$
7	$\langle \mathtt{sep} \rangle(\varphi, \psi) * \mathit{Atom}(\mathtt{x}_i) \Rightarrow (\varphi'_\alpha \vee \varphi'_{\alpha-1} \mathbin{-\!\!\circledast} \top)$	$\Rightarrow$**-Tr**, 4, 5, 6
8	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (\mathit{Atom}(\mathtt{x}_i) \mathbin{-\!\!\circledast} \langle \mathtt{sep} \rangle(\varphi, \psi) * \mathit{Atom}(\mathtt{x}_i))$	(‡)
9	$(\mathit{Atom}(\mathtt{x}_i) \mathbin{-\!\!\circledast} \langle \mathtt{sep} \rangle(\varphi, \psi) * \mathit{Atom}(\mathtt{x}_i)) \Rightarrow$ $(\mathit{Atom}(\mathtt{x}_i) \mathbin{-\!\!\circledast} (\varphi'_\alpha \vee \varphi'_{\alpha-1} \mathbin{-\!\!\circledast} \top))$	$\mathbf{(I^{-\!\!*}_{6.3.5})}$, 7
10	$\big(\mathit{Atom}(\mathtt{x}_i) \mathbin{-\!\!\circledast} (\varphi'_\alpha \vee \varphi'_{\alpha-1} \mathbin{-\!\!\circledast} \top)\big) \Rightarrow$ $(\mathit{Atom}(\mathtt{x}_i) * (\varphi'_\alpha \vee \varphi'_{\alpha-1}) \mathbin{-\!\!\circledast} \top)$	$\mathbf{(I^{-\!\!*}_{6.3.6})}$
11	$(\mathit{Atom}(\mathtt{x}_i) * (\varphi'_\alpha \vee \varphi'_{\alpha-1}) \mathbin{-\!\!\circledast} \top) \Rightarrow (\varphi \mathbin{-\!\!\circledast} \top)$	$\mathbf{(I^{-\!\!*}_{6.3.4})}$, 3
12	$\langle \mathtt{sep} \rangle(\varphi, \psi) \Rightarrow (\varphi \mathbin{-\!\!\circledast} \top)$	$\Rightarrow$**-Tr**, 8, 9, 10, 11

Figure 10: Proof of Lemma 6.2: the final derivation.

Lemma 6.2 in which φ and ψ are core types can be extended to arbitrary Boolean combinations of core formulae, as we show that the distributivity of $\mathbin{-\!\!\circledast}$ over disjunctions is provable in $\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})$. As a consequence of this development, we achieve the main result of the paper.

Theorem 6.5. *$\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})$ is sound and complete for $\mathsf{SL}(*, \mathbin{-\!\!*})$.*

Proof. Soundness of the proof system $\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})$ has been already established earlier, see Lemma 3.1. As far as the completeness proof is concerned, its structure is very similar to the proof of Theorem 5.6 except that we have to be able to handle the separating implication. In order to be self-contained, we reproduce some of its arguments albeit adapted to $\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})$.

We need to show that for every formula φ in $\mathsf{SL}(*, \mathbin{-\!\!*})$, there is a Boolean combination of core formulae ψ such that $\vdash_{\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})} \varphi \Leftrightarrow \psi$. In order to conclude the proof, when φ is valid for $\mathsf{SL}(*, \mathbin{-\!\!*})$, by soundness of $\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})$, we obtain that ψ is valid too and therefore $\vdash_{\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})} \psi$ as $\mathcal{H}_{\mathsf{C}}$ is a subsystem of $\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})$ and $\mathcal{H}_{\mathsf{C}}$ is complete by Theorem 4.3. By propositional reasoning, we get that $\vdash_{\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})} \varphi$.

In order to show that every formula φ has a provably equivalent Boolean combination of core formulae, we heavily rely on Corollary 5.5 and on Lemma 6.2. The proof is by simple induction on the number of occurrences of $*$ or $\mathbin{-\!\!*}$ in φ that are not involved in the definition of some core formula of the form $\mathtt{size} \geqslant \beta$ or $\mathtt{alloc}(\mathtt{x})$. For the base case, when φ has no occurrence of the separating connectives, $\mathtt{x} = \mathtt{y}$ and $\mathtt{x} \hookrightarrow \mathtt{y}$ are already core formulae, whereas $\mathtt{emp}$ is logically equivalent to $\neg \mathtt{size} \geqslant 1$.

Before performing the induction step, let us observe that in $\mathcal{H}_{\mathsf{C}}(*, \mathbin{-\!\!*})$, the replacement of provably equivalent formulae holds true, which is stated as follows:

R1 Let φ, φ' and ψ be formulae of $\mathsf{SL}(*, -\!\!*)$ such that $\vdash_{\mathcal{H}_\mathsf{C}(*,-\!\!*)} \varphi \Leftrightarrow \varphi'$. Then,

$$\vdash_{\mathcal{H}_\mathsf{C}(*,-\!\!*)} \psi[\varphi]_\rho \Rightarrow \psi[\varphi']_\rho$$

In order to prove **R1**, we are almost done as we have already shown **R0** in the proof of Theorem 5.6 and the same properties hold for $\mathsf{SL}(*, -\!\!*)$ though the language is richer.

As a direct consequence of the admissibility of the rules $\mathbf{(I^*_{6.3.4})}$ and $\mathbf{(I^*_{6.3.5})}$ from Lemma 6.3, the rules below are also admissible:

$$\frac{\varphi \Leftrightarrow \varphi'}{\varphi -\!\!* \psi \Leftrightarrow \varphi' -\!\!* \psi} \qquad \frac{\varphi \Leftrightarrow \varphi'}{\psi -\!\!* \varphi \Leftrightarrow \psi -\!\!* \varphi'}$$

We need the two rules as $-\!\!*$ is not commutative. Consequently, by structural induction on ψ, one can conclude that $\vdash_{\mathcal{H}_\mathsf{C}(*,-\!\!*)} \varphi \Leftrightarrow \varphi'$ implies $\vdash_{\mathcal{H}_\mathsf{C}(*,-\!\!*)} \psi[\varphi]_\rho \Rightarrow \psi[\varphi']_\rho$.

Now, assume φ is a formula in $\mathsf{SL}(*, -\!\!*)$. Without loss of generality, we can assume that the separating connectives in φ are restricted to $*$ and $-\!\!\circledast$ for the occurrences that are not related to abbreviations for core formulae. Indeed, $\psi' -\!\!\circledast \psi$ is a shortcut for $\neg(\psi' -\!\!* \neg\psi)$ and therefore one can replace every occurrence of $\psi' -\!\!* \psi$ by $\neg(\psi' -\!\!\circledast \neg\psi)$ assuming that ψ' and ψ are already of the appropriate shape. Such a replacement is possible thanks to **R1**.

Assume that φ is a formula in $\mathsf{SL}(*, -\!\!\circledast)$ with $n+1$ occurrences of $*$ or $-\!\!\circledast$ not involved in the definition of core formulae.

Let ψ be a subformula of φ (at the occurrence ρ) of the form $\psi_1 -\!\!\circledast \psi_2$ such that ψ_1 and ψ_2 are in $\mathsf{Bool}(\mathsf{Core}(\mathtt{X}, \alpha_1))$ and $\mathsf{Bool}(\mathsf{Core}(\mathtt{X}, \alpha_2))$, respectively. By propositional reasoning, one can show that there are formulae in disjunctive normal form $\psi_1^1 \vee \cdots \vee \psi_1^{n_1}$ and $\psi_2^1 \vee \cdots \vee \psi_2^{n_2}$ such that $\vdash_{\mathcal{H}_\mathsf{C}} \psi_i \Leftrightarrow \psi_i^1 \vee \cdots \vee \psi_i^{n_i}$ for $i \in \{1, 2\}$, and moreover every ψ_i^j's is a core type in $\mathsf{CoreTypes}(\mathtt{X}, \max(\mathrm{card}(\mathtt{X}), \alpha_1, \alpha_2))$. Again, by using propositional reasoning but this time establishing also distributivity of $\vee$ over $-\!\!\circledast$, we have

$$\vdash_{\mathcal{H}_\mathsf{C}(*,-\!\!*)} \psi_1 -\!\!\circledast \psi_2 \Leftrightarrow \bigvee_{j_1 \in [1,n_1], j_2 \in [1,n_2]} \psi_1^{j_1} -\!\!\circledast \psi_2^{j_2}.$$

We rely on Lemma 6.2, and conclude that there is a conjunction of core formulae ψ^{j_1,j_2} in $\mathsf{Conj}(\mathsf{Core}(\mathtt{X}, \max(\mathrm{card}(\mathtt{X}), \alpha_1, \alpha_2)))$ such that $\vdash_{\mathcal{H}_\mathsf{C}(*,-\!\!*)} \psi_1^{j_1} -\!\!\circledast \psi_2^{j_2} \Leftrightarrow \psi^{j_1,j_2}$. By propositional reasoning, we get

$$\vdash_{\mathcal{H}_\mathsf{C}(*,-\!\!*)} \psi_1 -\!\!\circledast \psi_2 \Leftrightarrow \bigvee_{j_1 \in [1,n_1], j_2 \in [1,n_2]} \psi^{j_1,j_2}.$$

Consequently (thanks to the property **R1**), we obtain

$$\vdash_{\mathcal{H}_\mathsf{C}(*,-\!\!*)} \varphi \Leftrightarrow \varphi[\bigvee_{j_1 \in [1,n_1], j_2 \in [1,n_2]} \psi^{j_1,j_2}]_\rho$$

Note that the right-hand side formula has n occurrences of the separating connnectives that are not involved in the definition of some core formula. The induction hypothesis applies, which concludes the proof.

The case when ψ is a subformula of φ (at the occurrence ρ) of the form $\psi_1 * \psi_2$ is treated as in the proof of Theorem 5.6 and therefore is omitted herein. □

7. Related work

In this section, we briefly compare our Hilbert-style proof system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ with existing proof systems for $\mathsf{SL}(*, -\!\!*)$, fragments or extensions and we recall a few landmark works proposing proof systems for abstract separation logics or for logics that are variants of Boolean BI. Those latter proof systems are not necessarily Hilbert-style and may contain labels or other similar machineries. So, this section completes the presentation of the context from Section 1 while pinpointing the main original features of our calculus. Finally, we also evoke several works that use the idea of axiomatising a fragment of a logic and to provide in the proof system means to transform any formula into an equivalent formula from that fragment. This is clearly similar to the approach we have followed, but we aim at picking examples from outside the realm of spatial and resource logics. In order to keep the length of this section reasonable, we limit ourselves to the main bibliographical entries but additional relevant works can be found in the cited materials.

Proof systems for quantifier-free separation logic. Surprisingly, as far as we know, sound and complete proof systems for $\mathsf{SL}(*, -\!\!*)$ are very rare and the only system we are aware of is a tableaux-based calculus from [GM10] with labelled formulae (each formula is enriched with a label to be interpreted by some heap) and with resource graphs to encode symbolically constraints between heap expressions (i.e. labels). Of course, translations from separation logics into logics or theories have been designed, see e.g. [CGH05, RISK16], but the finding of proof systems for $\mathsf{SL}(*, -\!\!*)$ with all Boolean connectives and the separating connectives $*$ and $-\!\!*$ has been quite challenging. Unlike [GM10], $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ uses only $\mathsf{SL}(*, -\!\!*)$ formulae and therefore can be viewed as a quite orthodox Hilbert-style calculus with no extra syntactic objects. In particular, $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ has no syntactic machinery to refer to heaps or to other semantical objects related to $\mathsf{SL}(*, -\!\!*)$. In [GM10], the resource graphs attached to the tableaux are designed to reason about heap constraints, and to provide control for designing strategies that lead to termination. Interestingly, the calculus in [GM10] is intended to be helpful to synthesize countermodels (which is a standard feature for labelled deduction systems [Gab96]) or to be extended to the first-order case, which is partly done in [GM10] but we know that completeness is theoretically impossible. Besides, a sound labelled sequent calculus for the first-order extension of $\mathsf{SL}(*, -\!\!*)$ is presented in [HGT15] but completeness for the sublogic $\mathsf{SL}(*, -\!\!*)$ is not established. The calculus in [HGT15] has also labels, which differs from our puristic approach. A complete sequent-style calculus for the symbolic heap fragment has been designed quite early in [BCO04] but does not deal with full $\mathsf{SL}(*, -\!\!*)$ (in particular it is not closed under Boolean connectives and does not contain the separating implication). A complexity-wise optimal decision procedure for the symbolic heap fragment is designed in [CHO$^+$11] based on a characterisation in terms of homomorphisms.

Frameworks for abstract separation logics. Bunched logics, such as the original bunched logic BI in [OP99], are known to be closely related to separation logics that can be viewed as concretisation of (Boolean) BI with models made of memory states, see e.g. [Pym02, Rey02, GM05, PSO18]. Actually, bunched logics come with different flavours, Boolean BI being considered as the genuine abstract version of $\mathsf{SL}(*, -\!\!*)$. Though Boolean BI has been shown undecidable in [LG13, BK14], a Hilbert-style axiomatisation can be found in [GLW06]. Our proof system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ inherits all the axiom schemas and inference rules for Boolean BI from [GLW06], which is expected as $\mathsf{SL}(*, -\!\!*)$ can be viewed as Boolean

BI on concrete heaps but with the notable difference of having built-in atomic formulae $\mathtt{x} = \mathtt{y}$ and $\mathtt{x} \hookrightarrow \mathtt{y}$. Bunched logics, such as Boolean BI, can be defined in several ways, for instance assuming classical or intuitionistic connectives, and in [Bro12], a unified proof theory based on display calculi [Bel82] is designed for a variety of four bunched logics, including Boolean BI (see also the nested sequent calculus for Boolean BI in [PSP13]). In display calculi, structural connectives enrich the sequent-style structures, providing a family of structural connectives accompanying the standard comma from sequent-style calculi. The main results in [Bro12] include cut-elimination, soundness and completeness. So, compared to our calculus $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$, the calculi in [Bro12] are designed for logics with more abstract semantical structures and owns a proof-theoretical machinery that does not include labels but instead complex structured sequents.

The quest for designing frameworks dedicated to classes of abstract separation logics have been pursued in several directions. For instance, models for Boolean BI are typically relational commutative monoids but properties can be added leading to a separation theory. In [BV14], a hybrid version of Boolean BI is introduced, called HyBBI, in which nominals (in the sense of hybrid modal logics, see e.g. [ABM01]) are added in order to be able to express rich standard properties in separation theory, such as cancellativity. Not only an Hilbert-style proof system is provided for HyBBI [BV14] but also a parametric completeness result is shown. More precisely, any extension of the proof system for HyBBI with a set of specific axioms is actually complete with respect to the class of models that satisfy the axioms, which is analogous to Sahlqvist's Theorem for modal logics [Sah75, BdRV01]. This provides a very general means to axiomatise variants of Boolean BI but at the cost of having the extra machinery for nominals. Moreover, as HyBBI and its extensions are abstract separation logics with no atomic formulae of the form $\mathtt{x} = \mathtt{y}$ or $\mathtt{x} \hookrightarrow \mathtt{y}$, the tools developed in [BV14] are of no help to design an Hilbert-style proof system for $\mathsf{SL}(*, -\!\!*)$ (except that its part dealing with Boolean BI is precisely borrowed from [GLW06] too).

Besides, in [HCGT18] labelled sequent calculi are designed for several abstract separation logics by considering different sets of properties. The sequents contain labelled formulae (a formula prefixed by a label to be interpreted as an abstract heap) as well as relational atoms to express relationships between abstract heaps. Though the framework in [HCGT18] is modular and very general to handle abstract separation logics, it is not tailored to separation logics with concrete semantics, see [HCGT18, Section 7] for possible future directions. In contrast, as explained already, the paper [HGT15] deals with first-order separation logic with concrete semantics and presents a sound labelled sequent calculus for it. Of course, the calculus cannot be complete but more importantly in the context of the current paper, completeness is not established for the quantifier-free fragment. In [HGT15], the sequents contain labelled formulae and relational atoms, similarly to [HCGT18] (see also [Hóu15]). Hence, this does not meet our requirements to have a pure axiomatisation in which only logical formulae from quantifier-free separation logic are allowed.

Modularity of the approaches from [Bro12, BV14, HCGT18] is further developed in the recent work [DP18, Doc19] by proposing a framework for labelled tableaux systems parametrised by the choice of separation theories (in the very sense of [BV14]). It is remarkable that the developments in [DP18, Doc19] are very general as it can handle separation theories that can be expressed in the rich class of so-called coherent first-order formulae, included in the first-order fragment Π_2. The first-order axioms are directly translated into inference rules. The calculi use labelled formulae (every formula is decorated by a sign and by a label) as well as constraints enforcing properties between worlds/resources.

Unlike [GM10], the reasoning about labels is not outsourced but handled directly by the calculus. As several works mentioned above, the framework in [DP18, Doc19] does not provide for free a proof system for $\mathsf{SL}(*, -\!\!*)$ (which might have been a close cousin of the one in [GM10]). More importantly, similarly to the works [GM10, BV14, HCGT18], the labelled tableaux systems handle syntactic objects referring to semantical concepts related to the abstract separation logics that go beyond the only presence of formulae. In a way, modularity of the approach prevents from having a puristic calculus for $\mathsf{SL}(*, -\!\!*)$, apart from the fact that $\mathsf{SL}(*, -\!\!*)$ is not part of the logics handled in [DP18].

Axiomatising knowledge logics with reduction axioms. In order to conclude this section, let us recall that the derivations in $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ are able to simulate the bottom-up elimination of separating connectives, leading to Boolean combinations of core formulae for which the system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ is also complete. As the core formulae are (simple) formulae in $\mathsf{SL}(*, -\!\!*)$, the axiomatisation provided by $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ uses only $\mathsf{SL}(*, -\!\!*)$ formulae and is complete for the full logic $\mathsf{SL}(*, -\!\!*)$ (and not only for Boolean combinations of core formulae). Note that as a by-product of our completeness proof for $\mathsf{SL}(*, -\!\!*)$, we get expressive completeness of $\mathsf{SL}(*, -\!\!*)$ with respect to Boolean combinations of core formulae, with a proof different from the developments in [Loz04a, BDL09, EIP19].

This general principle described above is familiar for axiomatising dynamic epistemic logics in which dynamic connectives might be eliminated with the help of so-called *reduction axioms*, see e.g. standard examples in [vDvdHK08, vB11, WC13, FVQ19]. In a nutshell, every formula containing a dynamic operator is provably reduced to a formula without such an operator. Completeness is then established thanks to the completeness of the underlying 'basic' language, A similar approach for the linear μ-calculus is recently presented in [Dou17] for which a form of constructive completeness is advocated, see also [Lüc18]. Hilbert-style axiomatisations following similar high-level principles for the modal separation logics MSL($*$,$\Diamond$) and MSL($*$,$\langle\neq\rangle$) introduced in [DF19], have been designed in [DFM19].

8. Conclusion

We presented a method to axiomatise internally quantifier-free separation logic $\mathsf{SL}(*, -\!\!*)$ based on the axiomatisation of Boolean combinations of core formulae (and even more precisely, based on the restricted fragment of core types). We designed the first proof system for $\mathsf{SL}(*, -\!\!*)$ that is completely internal and highlights the essential ingredients of the heaplet semantics. The fact that the calculus is internal simply means that the axioms and inference rules involve schemas instantiated by formulae in $\mathsf{SL}(*, -\!\!*)$ (no use of nominals, labels or other syntactic objects that are not $\mathsf{SL}(*, -\!\!*)$ formulae). Obviously, the Hilbert-style proof system presented in the paper is of theoretical interest, at least to grasp what are the essential features of $\mathsf{SL}(*, -\!\!*)$. Still, it remains to be seen whether applications are possible for designing decision procedures, for instance to feed provers with appropriate axiom instances to accelerate the proof search. Furthermore, we have not investigated whether the proof system $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ (see Figure 1) can be simplified without loosing completeness. This might be rewarding for using the calculus for other logics or for other applications. Most probably the most obvious part to study in that respect would be $\mathcal{H}_{\mathsf{C}}(*)$.

To provide further evidence that our method is robust, it is desirable to apply it to axiomatise other separation logics, for instance by adding the list segment predicate `ls` [BCO04] (or more generally user-defined inductive predicates) or by adding first-order quantification.

A key step in our approach is first to show that the logic admits a characterisation in terms of core formulae and such formulae need to be designed adequately. Of course, it is required that the set of valid formulae is recursively enumerable, which discards any attempt with $\mathsf{SL}(*, -\!\!*, \mathtt{ls})$ or with the first-order version of $\mathsf{SL}(*, -\!\!*)$ [DLM18a, BDL12]. The second part of the paper [DLM20] introduces an extension of $\mathsf{SL}(*, \mathtt{ls})$ and presents an axiomatisation with our method. More separation logics could be axiomatised that way, other good candidates are the version of separation logic with one individual variable studied in [DGLWM17] as well as the quantifier-free separation logic with general universes from [EIP19].

Acknowledgements. We would like to thank the anonymous reviewers for their numerous remarks and suggestions that help us to improve the quality of the document.

References

[ABM01] C. Areces, P. Blackburn, and M. Marx. Hybrid logics: characterization, interpolation and complexity. *The Journal of Symbolic Logic*, 66(3):977–1010, 2001.

[BCO04] J. Berdine, C. Calcagno, and P.W. O'Hearn. A decidable fragment of separation logic. In *FST&TCS'04*, volume 3328 of *LNCS*, pages 97–109. Springer, 2004.

[BDL09] R. Brochenin, S. Demri, and É. Lozes. Reasoning about sequences of memory states. *Annals of Pure and Applied Logic*, 161(3):305–323, 2009.

[BDL12] R. Brochenin, S. Demri, and É. Lozes. On the almighty wand. *Information and Computation*, 211:106–137, 2012.

[BdRV01] P. Blackburn, M. de Rijke, and Y. Venema. *Modal Logic*. Cambridge University Press, 2001.

[Bel82] N. Belnap. Display logic. *Journal of Philosophical Logic*, 11:375–417, 1982.

[BIP10] M. Bozga, R. Iosif, and S. Perarnau. Quantitative separation logic and programs with lists. *Journal of Automated Reasoning*, 45(2):131–156, 2010.

[BK14] J. Brotherston and M. Kanovich. Undecidability of propositional separation logic and its neighbours. *Journal of the Association for Computing Machinery*, 61(2), 2014.

[BK18] J. Brotherston and M. Kanovich. On the complexity of pointer arithmetic in separation logic. In *APLAS'18*, volume 11275 of *LNCS*, pages 329–349. Springer, 2018.

[Bro12] J. Brotherston. Bunched logics displayed. *Studia Logica*, 100(6):1223–1254, 2012.

[BV14] J. Brotherston and J. Villard. Parametric completeness for separation theories. In *POPL'14*, pages 453–464. ACM, 2014.

[CGH05] C. Calcagno, Ph. Gardner, and M. Hague. From separation logic to first-order logic. In *FoSSaCS'05*, volume 3441 of *LNCS*, pages 395–409. Springer, 2005.

[CHO+11] B. Cook, C. Haase, J. Ouaknine, M. Parkinson, and J. Worrell. Tractable reasoning in a fragment of separation logic. In *CONCUR'11*, volume 6901 of *LNCS*, pages 235–249. Springer, 2011.

[COY01] C. Calcagno, P.W. O'Hearn, and H. Yang. Computability and complexity results for a spatial assertion language for data structures. In *FST&TCS'01*, volume 2245 of *LNCS*, pages 108–119. Springer, 2001.

[DD15] S. Demri and M. Deters. Separation logics and modalities: A survey. *Journal of Applied Non-Classical Logics*, 25(1):50–99, 2015.

[DF19] S. Demri and R. Fervari. The power of modal separation logics. *Journal of Logic and Computation*, 29(8):1139–1184, 2019.

[DFM19] S. Demri, R. Fervari, and A. Mansutti. Axiomatising logics with separating conjunction and modalities. In *JELIA'19*, volume 11468 of *LNAI*, pages 692–708. Springer, 2019.

[DGLWM17] S. Demri, D. Galmiche, D. Larchey-Wendling, and D. Mery. Separation logic with one quantified variable. *Theory of Computing Systems*, 61:371–461, 2017.

[DLM18a] S. Demri, É. Lozes, and A. Mansutti. The effects of adding reachability predicates in propositional separation logic. In *FoSSaCS'18*, volume 10803 of *LNCS*, pages 476–493. Springer, 2018.

[DLM18b] S. Demri, É. Lozes, and A. Mansutti. The effects of adding reachability predicates in propositional separation logic. arXiv:1810.05410, October 2018. 44 pages. Long version of [DLM18a].

[DLM20] S. Demri, É. Lozes, and A. Mansutti. Internal calculi for separation logics. In *CSL'20*, Leibniz International Proceedings in Informatics, pages 19:1–19:18. Leibniz-Zentrum für Informatik, 2020.

[Doc19] S. Docherty. *Bunched logics: a uniform approach*. PhD thesis, University College London, 2019.

[Dou17] A. Doumane. Constructive completeness for the linear-time μ-calculus. In *LiCS'17*, pages 1–12. IEEE Computer Society, 2017.

[DP18] S. Docherty and D. Pym. Modular tableaux calculi for separation theories. In *FoSSaCS'18*, volume 10803 of *LNCS*, pages 441–458. Springer, 2018.

[EIP19] M. Echenim, R. Iosif, and N. Peltier. The Bernays-Schönfinkel-Ramsey class of separation logic on arbitrary domains. In *FoSSaCS'19*, volume 11425 of *LNCS*, pages 242–259. Springer, 2019.

[FVQ19] R. Fervari and F. R. Velázquez-Quesada. Introspection as an action in relational models. *Journal of Logical and Algebraic Methods in Programming*, 108:1–23, 2019.

[Gab96] D. Gabbay. *Labelled Deductive Systems*. Oxford University Press, 1996.

[GLW06] D. Galmiche and D. Larchey-Wending. Expressivity properties of boolean BI through relational models. In *FST&TCS'06*, volume 4337 of *LNCS*, pages 358–369. Springer, 2006.

[GM05] D. Galmiche and D. Mery. Characterizing provability in BI's pointer logic through resource graphs. In *LPAR'05*, volume 3835 of *LNCS*, pages 459–473. Springer, 2005.

[GM10] D. Galmiche and D. Méry. Tableaux and resource graphs for separation logic. *Journal of Logic and Computation*, 20(1):189–231, 2010.

[GvD06] V. Goranko and G. van Drimmelen. Complete axiomatization and decidability of alternating-time temporal logic. *Theoretical Computer Science*, 353(1-3):93–117, 2006.

[HCGT18] Z. Hóu, R. Clouston, R. Goré, and A. Tiu. Modular labelled sequent calculi for abstract separation logics. *ACM Transactions on Computational Logic*, 19(2):13:1–13:35, 2018.

[HGT15] Z. Hóu, R. Goré, and A. Tiu. Automated theorem proving for assertions in separation logic with all connectives. In *CADE'15*, volume 9195 of *LNCS*, pages 501–516. Springer, 2015.

[Hóu15] Z. Hóu. *Labelled sequent calculi and automated reasoning for assertions in separation logic*. PhD thesis, Australian National University, November 2015.

[IO01] S. Ishtiaq and P.W. O'Hearn. BI as an assertion language for mutable data structures. In *POPL'01*, pages 14–26. ACM, 2001.

[Kai95] R. Kaivola. Axiomatising linear time mu-calculus. In *CONCUR'95*, volume 962 of *LNCS*, pages 423–437. Springer, 1995.

[LG13] D. Larchey-Wendling and D. Galmiche. Nondeterministic phase semantics and the undecidability of Boolean BI. *ACM Transactions on Computational Logic*, 14(1), 2013.

[LMX16] K.G. Larsen, R. Mardare, and B. Xue. Probabilistic mu-calculus: Decidability and complete axiomatization. In *FST&TCS'16*, volume 65 of *LIPIcs*, pages 25:1–25:18. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

[Loz04a] É. Lozes. *Expressivité des Logiques Spatiales*. PhD thesis, ENS Lyon, 2004.

[Loz04b] É. Lozes. Separation logic preserves the expressive power of classical logic. In *SPACE'04*, 2004.

[Lüc18] M. Lück. Axiomatizations of team logics. *Annals of Pure and Applied Logic*, 169(9):928–969, 2018.

[Man18] A. Mansutti. Extending propositional separation logic for robustness properties. In *FST&TCS'18*, volume 122 of *LIPIcs*, pages 42:1–42:23. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

[Man20] A. Mansutti. *Reasoning with Separation Logics: Complexity, Expressive Power, Proof Systems*. PhD thesis, Université Paris-Saclay, December 2020.

[O'H12] P.W. O'Hearn. A primer on separation logic. In *Software Safety and Security: Tools for Analysis and Verification*, volume 33 of *NATO Science for Peace and Security Series*, pages 286–318, 2012.

[OP99] P.W. O'Hearn and D. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.

[PSO18] D. Pym, J. Spring, and P.W. O'Hearn. Why separation logic works. *Philosophy & Technology*, pages 1–34, 2018.

[PSP13] J. Park, J. Seo, and S. Park. A theorem prover for Boolean BI. In *POPL'13*, pages 219–232. ACM, 2013.

[PWZ13] R. Piskać, Th. Wies, and D. Zufferey. Automating separation logic using SMT. In *CAV'13*, volume 8044 of *LNCS*, pages 773–789. Springer, 2013.

[Pym02] D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic*. Kluwer Academic Publishers, 2002.

[Rey01] M. Reynolds. An axiomatization of full computation tree logic. *The Journal of Symbolic Logic*, 66(3):1011–1057, 2001.

[Rey02] J.C. Reynolds. Separation logic: a logic for shared mutable data structures. In *LiCS'02*, pages 55–74. IEEE, 2002.

[RISK16] A. Reynolds, R. Iosif, C. Serban, and T. King. A decision procedure for separation logic in SMT. In *ATVA'16*, volume 9938 of *LNCS*, pages 244–261, 2016.

[Sah75] H. Sahlqvist. Completeness and correspondence in the first and second order semantics for modal logics. In S. Kanger, editor, *3rd Scandinavian Logic Symposium, Uppsala, Sweden, 1973*, pages 110–143. North Holland, 1975.

[SV18] L. Schröder and Y. Venema. Completeness of flat coalgebraic fixpoint logics. *ACM Transactions on Computational Logic*, 19(1):4:1–4:34, 2018.

[vB11] J. van Benthem. *Logical Dynamics of Information and Interaction*. Cambridge University Press, 2011.

[vDvdHK08] H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamic Epistemic Logic*, volume 337 of *Synthese Library Series*. Springer, Dordrecht, 2008.

[Wal00] I. Walukiewicz. Completeness of Kozen's axiomatisation of the propositional μ-calculus. *Information and Computation*, 157(1–2):142–182, 2000.

[WC13] Y. Wang and Q. Cao. On axiomatizations of public announcement logic. *Synthese*, 190(Supplement-1):103–134, 2013.

[Yan01] H. Yang. *Local Reasoning for Stateful Programs*. PhD thesis, University of Illinois, Urbana-Champaign, 2001.

As in the rest of the paper, in the derivations below we use the following precedence between the various connectives of $\mathsf{SL}(*, -\!\!*)$: $\{\neg\} > \{\wedge, \vee, *\} > \{\Rightarrow, -\!\!*, \circledast\} > \{\Leftrightarrow\}$.

Appendix A. Proof of Lemma 5.2

Proof of $(\mathbf{I^*_{5.2.1}})$.

1	$\varphi \Rightarrow (\varphi \wedge \mathtt{x} \sim \mathtt{y}) \vee (\varphi \wedge \neg \mathtt{x} \sim \mathtt{y})$	PC
2	$\varphi * \psi \Rightarrow ((\varphi \wedge \mathtt{x} \sim \mathtt{y}) \vee (\varphi \wedge \neg \mathtt{x} \sim \mathtt{y})) * \psi$	$*$**-Intro**, 1
3	$((\varphi \wedge \mathtt{x} \sim \mathtt{y}) \vee (\varphi \wedge \neg \mathtt{x} \sim \mathtt{y})) * \psi \Rightarrow ((\varphi \wedge \mathtt{x} \sim \mathtt{y}) * \psi) \vee ((\varphi \wedge \neg \mathtt{x} \sim \mathtt{y}) * \psi)$	$\mathbf{(I^*_9)}$
4	$\varphi \wedge \neg \mathtt{x} \sim \mathtt{y} \Rightarrow \neg \mathtt{x} \sim \mathtt{y}$	PC
5	$\psi \Rightarrow \top$	PC
6	$(\varphi \wedge \neg \mathtt{x} \sim \mathtt{y}) * \psi \Rightarrow (\neg \mathtt{x} \sim \mathtt{y}) * \top$	$*$**-Ilr**, 4, 5
7	$(\neg \mathtt{x} \sim \mathtt{y}) * \top \Rightarrow \neg \mathtt{x} \sim \mathtt{y}$	$\mathbf{(A^*_{14})}$
8	$(\varphi \wedge \neg \mathtt{x} \sim \mathtt{y}) * \psi \Rightarrow \neg \mathtt{x} \sim \mathtt{y}$	$\Rightarrow$**-Tr**, 6, 7
9	$((\varphi \wedge \mathtt{x} \sim \mathtt{y}) * \psi) \vee ((\varphi \wedge \neg \mathtt{x} \sim \mathtt{y}) * \psi) \Rightarrow ((\varphi \wedge \mathtt{x} \sim \mathtt{y}) * \psi) \vee \neg \mathtt{x} \sim \mathtt{y}$	8, PC
10	$\varphi * \psi \Rightarrow ((\varphi \wedge \mathtt{x} \sim \mathtt{y}) * \psi) \vee \neg \mathtt{x} \sim \mathtt{y}$	$\Rightarrow$**-Tr**, 2, 3, 9
11	$\mathtt{x} \sim \mathtt{y} \wedge (\varphi * \psi) \Rightarrow (\varphi \wedge \mathtt{x} \sim \mathtt{y}) * \psi$	10, PC $\square$

Proof of $(\mathbf{I^*_{5.2.2}})$.

1	$\mathtt{alloc}(\mathtt{x}) \wedge \mathtt{x} = \mathtt{y} \Rightarrow \mathtt{alloc}(\mathtt{y})$	$\mathbf{(A^C_2)}$
2	$\mathtt{x} = \mathtt{y} \wedge ((\varphi \wedge \mathtt{alloc}(\mathtt{x})) * \psi) \Rightarrow ((\varphi \wedge \mathtt{alloc}(\mathtt{x}) \wedge \mathtt{x} = \mathtt{y}) * \psi)$	$\mathbf{(I^*_{5.2.1})}$
3	$(\varphi \wedge \mathtt{alloc}(\mathtt{x}) \wedge \mathtt{x} = \mathtt{y}) * \psi \Rightarrow (\varphi \wedge \mathtt{alloc}(\mathtt{y})) * \psi$	PC, $*$**-Intro**, 1
4	$\mathtt{x} = \mathtt{y} \wedge ((\varphi \wedge \mathtt{alloc}(\mathtt{x})) * \psi) \Rightarrow (\varphi \wedge \mathtt{alloc}(\mathtt{y})) * \psi$	$\Rightarrow$**-Tr**, 2, 3 $\square$

Proof of $(\mathbf{I^*_{5.2.3}})$.

1	$\psi \Rightarrow (\psi \wedge \mathtt{alloc}(\mathtt{x})) \vee (\psi \wedge \neg \mathtt{alloc}(\mathtt{x}))$	PC
2	$(\varphi \wedge \mathtt{alloc}(\mathtt{x})) * \psi \Rightarrow$ $(\varphi \wedge \mathtt{alloc}(\mathtt{x})) * ((\psi \wedge \mathtt{alloc}(\mathtt{x})) \vee (\psi \wedge \neg \mathtt{alloc}(\mathtt{x})))$	$\mathbf{(A^*_7)}$, $*$**-Intro**, 1
3	$(\varphi \wedge \mathtt{alloc}(\mathtt{x})) * ((\psi \wedge \mathtt{alloc}(\mathtt{x})) \vee (\psi \wedge \neg \mathtt{alloc}(\mathtt{x}))) \Rightarrow$ $((\varphi \wedge \mathtt{alloc}(\mathtt{x})) * (\psi \wedge \mathtt{alloc}(\mathtt{x}))) \vee ((\varphi \wedge \mathtt{alloc}(\mathtt{x})) * (\psi \wedge \neg \mathtt{alloc}(\mathtt{x})))$	$\mathbf{(A^*_7)}$, $\mathbf{(I^*_9)}$, 2
4	$\chi \wedge \mathtt{alloc}(\mathtt{x}) \Rightarrow \mathtt{alloc}(\mathtt{x})$	$(\chi \in \{\varphi, \psi\})$, PC
5	$(\varphi \wedge \mathtt{alloc}(\mathtt{x})) * (\psi \wedge \mathtt{alloc}(\mathtt{x})) \Rightarrow \mathtt{alloc}(\mathtt{x}) * \mathtt{alloc}(\mathtt{x})$	$*$**-Ilr**, 4
6	$\mathtt{alloc}(\mathtt{x}) * \mathtt{alloc}(\mathtt{x}) \Rightarrow \bot$	$\mathbf{(A^*_{13})}$
7	$(\varphi \wedge \mathtt{alloc}(\mathtt{x})) * (\psi \wedge \mathtt{alloc}(\mathtt{x})) \Rightarrow \bot$	$\Rightarrow$**-Tr**, 5, 6
8	$(\varphi \wedge \mathtt{alloc}(\mathtt{x})) * \psi \Rightarrow \bot \vee ((\varphi \wedge \mathtt{alloc}(\mathtt{x})) * (\psi \wedge \neg \mathtt{alloc}(\mathtt{x})))$	PC, 2, 3, 7

9	$(\varphi \wedge \mathtt{alloc(x)}) * \psi \Rightarrow (\varphi \wedge \mathtt{alloc(x)}) * (\psi \wedge \neg\mathtt{alloc(x)})$	PC, 8
10	$\varphi \wedge \mathtt{alloc(x)} \Rightarrow \varphi$	PC
11	$(\varphi \wedge \mathtt{alloc(x)}) * (\psi \wedge \neg\mathtt{alloc(x)}) \Rightarrow \varphi * (\psi \wedge \neg\mathtt{alloc(x)})$	$*$**-Intro**, 10
12	$(\varphi \wedge \mathtt{alloc(x)}) * \psi \Rightarrow \varphi * (\psi \wedge \neg\mathtt{alloc(x)})$	$\Rightarrow$**-Tr**, 9, 11 □

Proof of $\mathbf{(I^*_{5.2.4})}$.

1	$\varphi \Rightarrow (\varphi \wedge \mathtt{alloc(x)}) \vee (\varphi \wedge \neg\mathtt{alloc(x)})$	PC
2	$\varphi * \psi \Rightarrow \big((\varphi \wedge \mathtt{alloc(x)}) \vee (\varphi \wedge \neg\mathtt{alloc(x)})\big) * \psi$	$*$**-Intro**, 1
3	$\big((\varphi \wedge \mathtt{alloc(x)}) \vee (\varphi \wedge \neg\mathtt{alloc(x)})\big) * \psi \Rightarrow$ $((\varphi \wedge \mathtt{alloc(x)}) * \psi) \vee ((\varphi \wedge \neg\mathtt{alloc(x)}) * \psi)$	$\mathbf{(I^*_9)}$
4	$\varphi \wedge \mathtt{alloc(x)} \Rightarrow \mathtt{alloc(x)}$	PC
5	$\psi \Rightarrow \top$	PC
6	$(\varphi \wedge \mathtt{alloc(x)}) * \psi \Rightarrow (\mathtt{alloc(x)} * \top)$	$*$**-Ilr**, 4, 5
7	$\mathtt{alloc(x)} * \top \Rightarrow \mathtt{alloc(x)}$	$\mathbf{(I^*_{12})}$
8	$\varphi * \psi \Rightarrow \mathtt{alloc(x)} \vee ((\varphi \wedge \neg\mathtt{alloc(x)}) * \psi)$	PC, 2, 3, 6, 7
9	$\neg\mathtt{alloc(x)} \wedge (\varphi * \varphi) \Rightarrow (\varphi \wedge \neg\mathtt{alloc(x)}) * \psi$	PC, 8 □

Proof of $\mathbf{(I^*_{5.2.5})}$.

1	$\varphi \Rightarrow (\varphi \wedge \mathtt{alloc(x)}) \vee (\varphi \wedge \neg\mathtt{alloc(x)})$	PC
2	$\varphi * (\neg\mathtt{alloc(x)} \wedge \psi) \Rightarrow$ $((\varphi\wedge\mathtt{alloc(x)}) * (\psi\wedge\neg\mathtt{alloc(x)})) \vee ((\varphi\wedge\neg\mathtt{alloc(x)}) * (\psi\wedge\neg\mathtt{alloc(x)}))$	$*$**-Intro**, 1, $\mathbf{(I^*_9)}$
3	$\chi \wedge \neg\mathtt{alloc(x)} \Rightarrow \neg\mathtt{alloc(x)}$	$(\chi \in \{\varphi, \psi\})$, PC
4	$(\varphi \wedge \neg\mathtt{alloc(x)}) * (\psi \wedge \neg\mathtt{alloc(x)}) \Rightarrow \neg\mathtt{alloc(x)} * \neg\mathtt{alloc(x)}$	PC, $*$**-Ilr**, 3
5	$\neg\mathtt{alloc(x)} * \neg\mathtt{alloc(x)} \Rightarrow \neg\mathtt{alloc(x)}$	$\mathbf{(A^*_{15})}$
6	$\varphi * (\neg\mathtt{alloc(x)} \wedge \psi) \Rightarrow ((\varphi \wedge \mathtt{alloc(x)}) * (\psi \wedge \neg\mathtt{alloc(x)})) \vee \neg\mathtt{alloc(x)}$	PC, 2, 4, 5
7	$\mathtt{alloc(x)} \wedge (\varphi * (\neg\mathtt{alloc(x)} \wedge \psi)) \Rightarrow (\varphi \wedge \mathtt{alloc(x)}) * (\psi \wedge \neg\mathtt{alloc(x)})$	PC, 6 □

Proof of $\mathbf{(I^*_{5.2.6})}$.

1	$\varphi \wedge \mathtt{alloc(x)} \Rightarrow (\varphi \wedge \mathtt{alloc(x)} \wedge \mathtt{x} \hookrightarrow \mathtt{y}) \vee (\varphi \wedge \mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y})$	PC
2	$(\varphi \wedge \mathtt{alloc(x)}) * \psi \Rightarrow$ $\big((\varphi \wedge \mathtt{alloc(x)} \wedge \mathtt{x} \hookrightarrow \mathtt{y}) \vee (\varphi \wedge \mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y})\big) * \psi$	$*$**-Intro**, 1
3	$(\varphi \wedge \mathtt{alloc(x)}) * \psi \Rightarrow$ $((\varphi \wedge \mathtt{alloc(x)} \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi) \vee ((\varphi \wedge \mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}) * \psi)$	$\mathbf{(I^*_9)}$, $\Rightarrow$**-Tr**, 2
4	$\varphi \wedge \mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y} \Rightarrow \mathtt{alloc(x)} \wedge \neg\mathtt{x} \hookrightarrow \mathtt{y}$	PC

5	$\psi \Rightarrow \top$	PC
6	$(\varphi \wedge \mathtt{alloc(x)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y}) * \psi \Rightarrow (\mathtt{alloc(x)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y}) * \top$	$*$**-Ilr**
7	$(\mathtt{alloc(x)} \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y}) * \top \Rightarrow \neg \mathtt{x} \hookrightarrow \mathtt{y}$	$\mathbf{(A^*_{16})}$
8	$(\varphi \wedge \mathtt{alloc(x)}) * \psi \Rightarrow ((\varphi \wedge \mathtt{alloc(x)} \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi) \vee \neg \mathtt{x} \hookrightarrow \mathtt{y}$	PC, 3, 6, 7
9	$\mathtt{x} \hookrightarrow \mathtt{y} \wedge ((\mathtt{alloc(x)} \wedge \varphi) * \psi) \Rightarrow (\varphi \wedge \mathtt{alloc(x)} \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi$	PC, 8
10	$\varphi \wedge \mathtt{alloc(x)} \wedge \mathtt{x} \hookrightarrow \mathtt{y} \Rightarrow \varphi \wedge \mathtt{x} \hookrightarrow \mathtt{y}$	PC
11	$(\varphi \wedge \mathtt{alloc(x)} \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi \Rightarrow (\varphi \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi$	$*$**-Intro**, 10
12	$\mathtt{x} \hookrightarrow \mathtt{y} \wedge ((\mathtt{alloc(x)} \wedge \varphi) * \psi) \Rightarrow (\varphi \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi$	$\Rightarrow$**-Tr**, 9, 11 □

Proof of $\mathbf{(I^*_{5.2.7})}$. Similar to the proof of $\mathbf{(I^*_{5.2.4})}$, by replacing $\mathtt{alloc(x)}$ with $\mathtt{x} \hookrightarrow \mathtt{y}$.

1	$\varphi \Rightarrow (\varphi \wedge \mathtt{x} \hookrightarrow \mathtt{y}) \vee (\varphi \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y})$	PC
2	$\varphi * \psi \Rightarrow ((\varphi \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi) \vee ((\varphi \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y}) * \psi)$	$*$**-Intro**, 1, $\mathbf{(I^*_9)}$
3	$\varphi \wedge \mathtt{x} \hookrightarrow \mathtt{y} \Rightarrow \mathtt{x} \hookrightarrow \mathtt{y}$	PC
4	$\psi \Rightarrow \top$	PC
5	$(\varphi \wedge \mathtt{x} \hookrightarrow \mathtt{y}) * \psi \Rightarrow (\mathtt{x} \hookrightarrow \mathtt{y} * \top)$	$*$**-Ilr**, 3, 4
6	$\mathtt{x} \hookrightarrow \mathtt{y} * \top \Rightarrow \mathtt{x} \hookrightarrow \mathtt{y}$	$\mathbf{(A^*_{14})}$
7	$\varphi * \psi \Rightarrow \mathtt{x} \hookrightarrow \mathtt{y} \vee ((\varphi \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y}) * \psi)$	PC, 2, 5, 6
8	$\neg \mathtt{x} \hookrightarrow \mathtt{y} \wedge (\varphi * \psi) \Rightarrow (\varphi \wedge \neg \mathtt{x} \hookrightarrow \mathtt{y}) * \psi$	PC, 7 □

Appendix B. Derivation of the size formulae required for Lemma 5.4

In this appendix, we show the derivations in $\mathcal{H}_{\mathsf{C}}(*)$ of $\mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} \geqslant \beta_2$ and $\mathtt{size} = \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} = \beta_2$, which are required for the proof of Lemma 5.4.

The derivation of $\mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} \geqslant \beta_2$ is proven by induction on β_1. The derivation for the base case $\beta_1 = 0$ is:

1	$\mathtt{size} \geqslant \beta_2 \Rightarrow \mathtt{emp} * \mathtt{size} \geqslant \beta_2$	$\mathbf{(A^*_{11})}$
2	$\mathtt{emp} \Rightarrow \mathtt{size} \geqslant 0 \wedge \neg \mathtt{size} \geqslant 1$	PC, def. of $\mathtt{size} \geqslant 1$
3	$\mathtt{emp} * \mathtt{size} \geqslant \beta_2 \Rightarrow \mathtt{size} = 0 * \mathtt{size} \geqslant \beta_2$	$*$**-Intro**, 2, def. of $\mathtt{size} = 0$
4	$\mathtt{size} \geqslant \beta_2 \Rightarrow \mathtt{size} = 0 * \mathtt{size} \geqslant \beta_2$	$\Rightarrow$**-Tr**, 1, 3

For the induction step, let us suppose the formula to be derivable for a certain β_1, and let us prove that it is also derivable for $\beta_1 + 1$.

1	$\mathtt{size} \geqslant \beta_1 + 1 + \beta_2 \Rightarrow \mathtt{size} \geqslant 1 * \mathtt{size} \geqslant \beta_1 + \beta_2$	def. of $\mathtt{size} \geqslant \beta$, $\mathbf{(A^*_7)}$, $\mathbf{(A^*_8)}$
2	$\mathtt{size} \geqslant 1 \Rightarrow \mathtt{size} = 1 * \top$	$\mathbf{(A^*_{18})}$, def. of $\mathtt{size} \geqslant 1$
3	$\mathtt{size} \geqslant 1 * \mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow$ $(\mathtt{size} = 1 * \top) * \mathtt{size} \geqslant \beta_1 + \beta_2$	$*$**-Intro**, 2

4	$(\mathtt{size} = 1 * \top) * \mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow$ $\mathtt{size} = 1 * \mathtt{size} \geqslant \beta_1 + \beta_2$	PC, $\mathbf{(A^*_7)}$, $\mathbf{(A^*_8)}$, $\mathbf{(A^*_{14})}$
5	$\mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} \geqslant \beta_2$	Induction Hypothesis
6	$\mathtt{size} = 1 * \mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow$ $(\mathtt{size} = 1 * \mathtt{size} = \beta_1) * \mathtt{size} \geqslant \beta_2$	$\mathbf{(A^*_7)}$, $*$**-Intro**, $\mathbf{(A^*_8)}$
7	$\mathtt{size} = \widetilde{\beta} \Rightarrow \mathtt{size} \geqslant \widetilde{\beta}$	PC, def. of $\mathtt{size} = \widetilde{\beta}$
8	$\mathtt{size} = \widetilde{\beta} \Rightarrow \neg\mathtt{size} \geqslant \widetilde{\beta} + 1$	PC, def. of $\mathtt{size} = \widetilde{\beta}$
9	$\mathtt{size} = 1 * \mathtt{size} = \beta_1 \Rightarrow \mathtt{size} \geqslant 1 * \mathtt{size} \geqslant \beta_1$	$*$**-Ilr**, 7
10	$\mathtt{size} = 1 * \mathtt{size} = \beta_1 \Rightarrow \neg\mathtt{size} \geqslant 2 * \neg\mathtt{size} \geqslant \beta_1 + 1$	$*$**-Ilr**, 8
11	$\mathtt{size} \geqslant 1 * \mathtt{size} \geqslant \beta_1 \Rightarrow \mathtt{size} \geqslant \beta_1 + 1$	def. of $\mathtt{size} \geqslant \beta$, $\mathbf{(A^*_7)}$, $\mathbf{(A^*_8)}$
12	$\neg\mathtt{size} \geqslant 2 * \neg\mathtt{size} \geqslant \beta_1 + 1 \Rightarrow \neg\mathtt{size} \geqslant \beta_1 + 2$	$\mathbf{(A^*_{19})}$
13	$\mathtt{size} = 1 * \mathtt{size} = \beta_1 \Rightarrow \mathtt{size} = \beta_1 + 1$	PC, 9–12, def. of $\mathtt{size} = \beta_1$
14	$(\mathtt{size} = 1 * \mathtt{size} = \beta_1) * \mathtt{size} \geqslant \beta_2 \Rightarrow$ $\mathtt{size} = \beta_1 + 1 * \mathtt{size} \geqslant \beta_2$	$*$**-Intro**, 13
15	$\mathtt{size} \geqslant \beta_1 + 1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 + 1 * \mathtt{size} \geqslant \beta_2$	$\Rightarrow$**-Tr**, 1, 3, 4, 6, 14

The derivation of the formula $\mathtt{size} = \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} = \beta_2$ is provided below.

1	$\mathtt{size} = \beta_1 + \beta_2 \Rightarrow \mathtt{size} \geqslant \beta_1 + \beta_2$	PC, def. of $\mathtt{size} = \beta$
2	$\mathtt{size} \geqslant \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} \geqslant \beta_2$	Previously derived
3	$\mathtt{size} \geqslant \beta_2 \Rightarrow (\mathtt{size} \geqslant \beta_2 \wedge \mathtt{size} \geqslant \beta_2 + 1) \vee \mathtt{size} = \beta_2$	PC, def. of $\mathtt{size} = \beta_2$
4	$\mathtt{size} = \beta_1 * \mathtt{size} \geqslant \beta_2 \Rightarrow$ $\mathtt{size} = \beta_1 * ((\mathtt{size} \geqslant \beta_2 \wedge \mathtt{size} \geqslant \beta_2 + 1) \vee \mathtt{size} = \beta_2)$	$\mathbf{(A^*_7)}$, $*$**-Intro**, 3
5	$\mathtt{size} = \beta_1 * ((\mathtt{size} \geqslant \beta_2 \wedge \mathtt{size} \geqslant \beta_2 + 1) \vee \mathtt{size} = \beta_2) \Rightarrow$ $(\mathtt{size} = \beta_1 * (\mathtt{size} \geqslant \beta_2 \wedge \mathtt{size} \geqslant \beta_2 + 1)) \vee (\mathtt{size} = \beta_1 * \mathtt{size} = \beta_2)$	$\mathbf{(A^*_7)}$, $\mathbf{(I^*_9)}$
6	$\mathtt{size} \geqslant \widetilde{\beta} \wedge \chi \Rightarrow \mathtt{size} \geqslant \widetilde{\beta}$	PC
7	$\mathtt{size} = \beta_1 * (\mathtt{size} \geqslant \beta_2 \wedge \mathtt{size} \geqslant \beta_2 + 1) \Rightarrow$ $\mathtt{size} \geqslant \beta_1 * \mathtt{size} \geqslant \beta_2 + 1$	PC, $*$**-Ilr**, 6
8	$\mathtt{size} \geqslant \beta_1 * \mathtt{size} \geqslant \beta_2 + 1 \Rightarrow \mathtt{size} \geqslant \beta_1 + \beta_2 + 1$	$\mathbf{(A^*_7)}$, $\mathbf{(A^*_8)}$
9	$\mathtt{size} = \beta_1 * (\mathtt{size} \geqslant \beta_2 \wedge \mathtt{size} \geqslant \beta_2 + 1) \Rightarrow \mathtt{size} \geqslant \beta_1 + \beta_2 + 1$	$\Rightarrow$**-Tr**, 7, 8
10	$\mathtt{size} = \beta_1 * ((\mathtt{size} \geqslant \beta_2 \wedge \mathtt{size} \geqslant \beta_2 + 1) \vee \mathtt{size} = \beta_2) \Rightarrow$ $\mathtt{size} \geqslant \beta_1 + \beta_2 + 1 \vee (\mathtt{size} = \beta_1 * \mathtt{size} = \beta_2)$	PC, 5, 9
11	$\mathtt{size} = \beta_1 + \beta_2 \Rightarrow \mathtt{size} \geqslant \beta_1 + \beta_2 + 1 \vee (\mathtt{size} = \beta_1 * \mathtt{size} = \beta_2)$	$\Rightarrow$**-Tr**, 1, 2, 4, 10
12	$\mathtt{size} = \beta_1 + \beta_2 \Rightarrow \neg\mathtt{size} \geqslant \beta_1 + \beta_2 + 1$	PC, def. of $\mathtt{size} = \beta$
13	$\mathtt{size} = \beta_1 + \beta_2 \Rightarrow \mathtt{size} = \beta_1 * \mathtt{size} = \beta_2$	PC, 11, 12

Appendix C. Proof of Lemma 6.1

Proof of $\mathbf{(I^*_9)}$.

1	$(\varphi * \chi) \Rightarrow (\varphi * \chi) \vee (\psi * \chi)$	PC
2	$(\psi * \chi) \Rightarrow (\varphi * \chi) \vee (\psi * \chi)$	PC
3	$\varphi \Rightarrow (\chi \mathrel{-\!\!*} (\varphi * \chi) \vee (\psi * \chi))$	$*$**-Adj**, 1
4	$\psi \Rightarrow (\chi \mathrel{-\!\!*} (\varphi * \chi) \vee (\psi * \chi))$	$*$**-Adj**, 2
5	$\varphi \vee \psi \Rightarrow (\chi \mathrel{-\!\!*} (\varphi * \chi) \vee (\psi * \chi))$	PC, 3, 4
6	$(\varphi \vee \psi) * \chi \Rightarrow (\varphi * \chi) \vee (\psi * \chi)$	$-\!\!*$**-Adj**, 5 □

Proof of $\mathbf{(I^*_{10})}$. The axiom $\mathbf{(I^*_{10})}$ is provable by $*$**-Adj**. Indeed, proving $(\bot * \varphi) \Rightarrow \bot$ reduces to proving $\bot \Rightarrow (\varphi \mathrel{-\!\!*} \bot)$. The latter is a tautology by propositional reasoning. □

Proof of $\mathbf{(I^*_{12})}$.

1	$\bot * \top \Rightarrow \bot$	$\mathbf{(I^*_{10})}$
2	$(\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot) \Rightarrow (\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot)$	PC
3	$(\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot) * \mathtt{x} \hookrightarrow \mathtt{x} \Rightarrow \bot$	$-\!\!*$**-Adj**, 2
4	$\mathtt{x} \hookrightarrow \mathtt{x} * (\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot) \Rightarrow (\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot) * \mathtt{x} \hookrightarrow \mathtt{x}$	$\mathbf{(A^*_7)}$
5	$\mathtt{x} \hookrightarrow \mathtt{x} * (\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot) \Rightarrow \bot$	$\Rightarrow$**-Tr**, 4, 3
6	$(\mathtt{x} \hookrightarrow \mathtt{x} * (\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot)) * \top \Rightarrow \bot * \top$	$*$**-Intro**, 5
7	$((\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot) * \top) * (\mathtt{x} \hookrightarrow \mathtt{x}) \Rightarrow (\mathtt{x} \hookrightarrow \mathtt{x} * (\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot)) * \top$	$\mathbf{(A^*_7)}$, $\mathbf{(A^*_8)}$
8	$((\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot) * \top) * (\mathtt{x} \hookrightarrow \mathtt{x}) \Rightarrow \bot$	$\Rightarrow$**-Tr**, 7, 6, 1
9	$(\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot) * \top \Rightarrow (\mathtt{x} \hookrightarrow \mathtt{x} \mathrel{-\!\!*} \bot)$	$*$**-Adj**, 8
10	$\mathtt{alloc}(\mathtt{x}) * \top \Rightarrow \mathtt{alloc}(\mathtt{x})$	Def. $\mathtt{alloc}(\mathtt{x})$, 9 □

Appendix D. Proof of Lemma 6.3

Proof of $\mathbf{(I^{-\!\!*}_{6.3.1})}$.

1	$\bot * \top \Rightarrow \bot$	$\mathbf{(I^*_{10})}$	4	$\top \Rightarrow (\bot \mathrel{-\!\!*} \neg\varphi)$	$\mathbf{(A^*_7)}$, $*$**-Adj**
2	$\bot \Rightarrow \neg\varphi$	PC	5	$\top \Rightarrow \neg(\bot \mathbin{-\!\!\circledast} \varphi)$	Def. $-\!\!\circledast$, PC
3	$\bot * \top \Rightarrow \neg\varphi$	$\Rightarrow$**-Tr**, 1, 2	6	$(\bot \mathbin{-\!\!\circledast} \varphi) \Rightarrow \bot$	5, PC □

Proof of $\mathbf{(I^{-\!\!*}_{6.3.2})}$.

1	$\top * \varphi \Rightarrow \top$	PC	3	$\neg(\varphi \mathrel{-\!\!*} \top) \Rightarrow \bot$	PC, 2
2	$\top \Rightarrow (\varphi \mathrel{-\!\!*} \top)$	$*$**-Adj**	4	$(\varphi \mathbin{-\!\!\circledast} \bot) \Rightarrow \bot$	Def. $-\!\!\circledast$, PC

Note that implicitly, we have assumed that we can replace $\neg\top$ by $\bot$ in the scope of $\mathrel{-\!\circledast}$ or $-\!\!*$, which is possible as the replacement of equivalents holds in the calculus $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$ (see e.g. the proof of Theorem 6.5). □

Proof of $(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.3}})$.

1	$(\varphi -\!\!* \psi) \Rightarrow (\varphi -\!\!* \psi)$	PC
2	$(\varphi -\!\!* \psi) * \varphi \Rightarrow \psi$	$-\!\!*$**-Adj**, 1
3	$\varphi * (\varphi -\!\!* \psi) \Rightarrow (\varphi -\!\!* \psi) * \varphi$	$(\mathbf{A}^{*}_{\mathbf{7}})$
4	$\varphi * (\varphi -\!\!* \psi) \Rightarrow \psi$	$\Rightarrow$**-Tr**, 3, 2 □

Proof of $(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.4}})$.

1	$\varphi \Rightarrow \psi$	Hypothesis
2	$\psi * (\psi -\!\!* \neg\chi) \Rightarrow \neg\chi$	$(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.3}})$
3	$(\psi -\!\!* \neg\chi) * \varphi \Rightarrow \varphi * (\psi -\!\!* \neg\chi)$	$(\mathbf{A}^{*}_{\mathbf{7}})$
4	$\varphi * (\psi -\!\!* \neg\chi) \Rightarrow \psi * (\psi -\!\!* \neg\chi)$	$*$**-Intro**, 1
5	$\varphi * (\psi -\!\!* \neg\chi) \Rightarrow \neg\chi$	$\Rightarrow$**-Tr**, 2, 4
6	$(\psi -\!\!* \neg\chi) * \varphi \Rightarrow \neg\chi$	$\Rightarrow$**-Tr**, 3, 5
7	$\psi -\!\!* \neg\chi \Rightarrow \varphi -\!\!* \neg\chi$	$*$**-Adj**, 6
8	$\neg(\varphi -\!\!* \neg\chi) \Rightarrow \neg(\psi -\!\!* \neg\chi)$	PC, 7
9	$(\varphi \mathrel{-\!\circledast} \chi) \Rightarrow (\psi \mathrel{-\!\circledast} \chi)$	Def. $\mathrel{-\!\circledast}$, 8 □

Proof of $(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.5}})$.

1	$\varphi \Rightarrow \psi$	Hypothesis
2	$\neg\psi \Rightarrow \neg\varphi$	PC, 1
3	$\chi * (\chi -\!\!* \neg\psi) \Rightarrow \neg\psi$	$(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.3}})$
4	$\chi * (\chi -\!\!* \neg\psi) \Rightarrow \neg\varphi$	$\Rightarrow$**-Tr**, 3, 2
5	$(\chi -\!\!* \neg\psi) * \chi \Rightarrow \chi * (\chi -\!\!* \neg\psi)$	$(\mathbf{A}^{*}_{\mathbf{7}})$
6	$(\chi -\!\!* \neg\psi) * \chi \Rightarrow \neg\varphi$	$\Rightarrow$**-Tr**, 4, 5
7	$(\chi -\!\!* \neg\psi) \Rightarrow (\chi -\!\!* \neg\varphi)$	$*$**-Adj**, 6
8	$\neg(\chi -\!\!* \neg\varphi) \Rightarrow \neg(\chi -\!\!* \neg\psi)$	PC, 7
9	$(\chi \mathrel{-\!\circledast} \varphi) \Rightarrow (\chi \mathrel{-\!\circledast} \psi)$	Def. $\mathrel{-\!\circledast}$ □

Proof of $(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.6}})$. By definition of the septraction operator $\mathrel{-\!\circledast}$, $(\mathbf{I}^{-\!\!*}_{\mathbf{6.3.6}})$ is equivalent to $\varphi -\!\!* (\psi -\!\!* \neg\chi)) \Leftrightarrow (\varphi * \psi) -\!\!* \neg\chi$. This equivalence is provable in $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$, thanks to the adjunction rules, as we now show.

1	$(\varphi * \psi) * (\varphi * \psi \mathrel{-\!\!*} \neg\chi) \Rightarrow \neg\chi$	$\mathbf{(I^{-*}_{6.3.3})}$
2	$\psi * (\varphi * (\varphi * \psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow \neg\chi$	$\mathbf{(A^{*}_{7})}$, $\mathbf{(A^{*}_{8})}$, 1
3	$\varphi * (\varphi * \psi \mathrel{-\!\!*} \neg\chi) \Rightarrow (\psi \mathrel{-\!\!*} \neg\chi)$	$*$**-Adj**, 2
4	$(\varphi * \psi \mathrel{-\!\!*} \neg\chi) \Rightarrow (\varphi \mathrel{-\!\!*} (\psi \mathrel{-\!\!*} \neg\chi))$	$*$**-Adj**, 3, $\mathbf{(A^{*}_{7})}$
5	$\varphi * (\varphi \mathrel{-\!\!*} (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow (\psi \mathrel{-\!\!*} \neg\chi)$	$\mathbf{(I^{-*}_{6.3.3})}$
6	$\psi * \varphi * (\varphi \mathrel{-\!\!*} (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow \neg\chi$	$\mathrel{-\!\!*}$**-Adj**, 5, $\mathbf{(A^{*}_{7})}$, $\mathbf{(A^{*}_{8})}$
7	$(\varphi * \psi) * (\varphi \mathrel{-\!\!*} (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow \neg\chi$	$\mathbf{(A^{*}_{7})}$, $\mathbf{(A^{*}_{8})}$, 6
8	$(\varphi \mathrel{-\!\!*} (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow (\varphi * \psi \mathrel{-\!\!*} \neg\chi)$	$*$**-Adj**, 7
9	$\varphi \mathrel{-\!\!*} (\psi \mathrel{-\!\!*} \neg\chi) \Leftrightarrow (\varphi * \psi) \mathrel{-\!\!*} \neg\chi$	PC, 4, 8 □

Proof of $\mathbf{(I^{-*}_{6.3.7})}$. We derive each implication separately.

1	$(\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi) \Rightarrow (\psi \mathrel{-\!\!*} \neg\chi)$	PC
2	$\psi * ((\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow \psi * (\psi \mathrel{-\!\!*} \neg\chi)$	$*$**-Ilr**, 1
3	$(\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi) \Rightarrow (\varphi \mathrel{-\!\!*} \neg\chi)$	PC
4	$\varphi * ((\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow \varphi * (\varphi \mathrel{-\!\!*} \neg\chi)$	$*$**-Ilr**, 3
5	$\varphi * (\varphi \mathrel{-\!\!*} \neg\chi) \Rightarrow \neg\chi$	$\mathbf{(I^{-*}_{6.3.3})}$
6	$\psi * (\psi \mathrel{-\!\!*} \neg\chi) \Rightarrow \neg\chi$	$\mathbf{(I^{-*}_{6.3.3})}$
7	$\psi * ((\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow \neg\chi$	$\Rightarrow$**-Tr**, 2, 6
8	$\varphi * ((\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow \neg\chi$	$\Rightarrow$**-Tr**, 4, 5
9	$(\varphi \vee \psi) * ((\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow$ $(\varphi * (\varphi \mathrel{-\!\!*} \neg\chi \wedge \psi \mathrel{-\!\!*} \neg\chi)) \vee (\psi * (\varphi \mathrel{-\!\!*} \neg\chi \wedge \psi \mathrel{-\!\!*} \neg\chi))$	$\mathbf{(I^{*}_{9})}$
10	$(\varphi \vee \psi) * ((\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi)) \Rightarrow \neg\chi$	PC, 7, 8, 9
11	$((\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi)) * (\varphi \vee \psi) \Rightarrow (\varphi \vee \psi) * ((\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi))$	$\mathbf{(A^{*}_{7})}$
12	$((\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi)) * (\varphi \vee \psi) \Rightarrow \neg\chi$	$\Rightarrow$**-Tr**, 12, 10
13	$(\varphi \mathrel{-\!\!*} \neg\chi) \wedge (\psi \mathrel{-\!\!*} \neg\chi) \Rightarrow (\varphi \vee \psi \mathrel{-\!\!*} \neg\chi)$	$*$**-Adj**, 12
14	$\neg(\varphi \vee \psi \mathrel{-\!\!*} \neg\chi) \Rightarrow \neg(\varphi \mathrel{-\!\!*} \neg\chi) \vee \neg(\psi \mathrel{-\!\!*} \neg\chi)$	PC, 13
15	$(\varphi \vee \psi \mathbin{-\!\!\circledast} \chi) \Rightarrow (\varphi \mathbin{-\!\!\circledast} \chi) \vee (\psi \mathbin{-\!\!\circledast} \chi)$	Def. $-\!\!\circledast$, 14

The derivation of the other implication can be found below.

1	$\varphi \Rightarrow \varphi \vee \psi$	PC
2	$\psi \Rightarrow \varphi \vee \psi$	PC
3	$(\varphi \mathbin{-\!\!\circledast} \chi) \Rightarrow (\varphi \vee \psi \mathbin{-\!\!\circledast} \chi)$	$\mathbf{(I^{-*}_{6.3.4})}$, 1
4	$(\psi \mathbin{-\!\!\circledast} \chi) \Rightarrow (\varphi \vee \psi \mathbin{-\!\!\circledast} \chi)$	$\mathbf{(I^{-*}_{6.3.4})}$, 2
5	$(\psi \mathbin{-\!\!\circledast} \chi) \vee (\varphi \mathbin{-\!\!\circledast} \chi) \Rightarrow (\varphi \vee \psi \mathbin{-\!\!\circledast} \chi)$	PC, 3, 4 □

Proof of $(\mathbf{I^{-\!\!*}_{6.3.8}})$. We handle each implication separately, and we follow a pattern similar to the one used in the proof of $(\mathbf{I^{-\!\!*}_{6.3.7}})$.

1	$\chi * (\chi \mathrel{-\!\!*} \neg\varphi) \Rightarrow \neg\varphi$	$(\mathbf{I^{-\!\!*}_{6.3.3}})$
2	$(\chi \mathrel{-\!\!*} \neg\varphi) \wedge (\chi \mathrel{-\!\!*} \neg\psi) \Rightarrow \chi \mathrel{-\!\!*} \neg\varphi$	PC
3	$\chi * ((\chi \mathrel{-\!\!*} \neg\varphi) \wedge (\chi \mathrel{-\!\!*} \neg\psi)) \Rightarrow \chi * (\chi \mathrel{-\!\!*} \neg\varphi)$	$*$**-Ilr**,2
4	$\chi * ((\chi \mathrel{-\!\!*} \neg\varphi) \wedge (\chi \mathrel{-\!\!*} \neg\psi)) \Rightarrow \neg\varphi$	$\Rightarrow$**-Tr**, 3, 1
5	$\chi * (\chi \mathrel{-\!\!*} \neg\psi) \Rightarrow \neg\psi$	$(\mathbf{I^{-\!\!*}_{6.3.3}})$
6	$(\chi \mathrel{-\!\!*} \neg\varphi) \wedge (\chi \mathrel{-\!\!*} \neg\psi) \Rightarrow (\chi \mathrel{-\!\!*} \neg\psi)$	PC
7	$\chi * ((\chi \mathrel{-\!\!*} \neg\varphi) \wedge (\chi \mathrel{-\!\!*} \neg\psi)) \Rightarrow \chi * (\chi \mathrel{-\!\!*} \neg\psi)$	$*$**-Ilr**,6
8	$\chi * ((\chi \mathrel{-\!\!*} \neg\varphi) \wedge (\chi \mathrel{-\!\!*} \neg\psi)) \Rightarrow \neg\psi$	$\Rightarrow$**-Tr**, 7, 5
9	$\chi * ((\chi \mathrel{-\!\!*} \neg\varphi) \wedge (\chi \mathrel{-\!\!*} \neg\psi)) \Rightarrow \neg(\varphi \vee \psi)$	PC, 4, 8
10	$((\chi \mathrel{-\!\!*} \neg\varphi) \wedge (\chi \mathrel{-\!\!*} \neg\psi)) * \chi \Rightarrow \neg(\varphi \vee \psi)$	$(\mathbf{A^*_7})$ + $\Rightarrow$**-Tr**, 9
11	$(\chi \mathrel{-\!\!*} \neg\varphi) \wedge (\chi \mathrel{-\!\!*} \neg\psi) \Rightarrow (\chi \mathrel{-\!\!*} \neg(\varphi \vee \psi))$	$*$**-Adj**, 10
12	$\neg(\chi \mathrel{-\!\!*} \neg(\varphi \vee \psi)) \Rightarrow \neg(\chi \mathrel{-\!\!*} \neg\varphi) \vee \neg(\chi \mathrel{-\!\!*} \neg\psi)$	PC, 11
13	$(\chi \mathrel{-\!\!\circledast} (\varphi \vee \psi)) \Rightarrow (\chi \mathrel{-\!\!\circledast} \varphi) \vee (\chi \mathrel{-\!\!\circledast} \psi)$	Def. $-\!\!\circledast$, 12

The derivation of the other implication can be found below.

1	$\varphi \Rightarrow \varphi \vee \psi$	PC
2	$\psi \Rightarrow \varphi \vee \psi$	PC
3	$(\chi \mathrel{-\!\!\circledast} \varphi) \Rightarrow (\chi \mathrel{-\!\!\circledast} \varphi \vee \psi)$	$(\mathbf{I^{-\!\!*}_{6.3.5}})$, 1
4	$(\chi \mathrel{-\!\!\circledast} \psi) \Rightarrow (\chi \mathrel{-\!\!\circledast} \varphi \vee \psi)$	$(\mathbf{I^{-\!\!*}_{6.3.5}})$, 2
5	$(\chi \mathrel{-\!\!\circledast} \varphi) \vee (\chi \mathrel{-\!\!\circledast} \psi) \Rightarrow (\chi \mathrel{-\!\!\circledast} \varphi \vee \psi)$	PC, 3, 4 $\square$

Proof of $(\mathbf{I^{-\!\!*}_{6.3.9}})$.

1	$\varphi * (\varphi \mathrel{-\!\!*} \chi) \Rightarrow \chi$	$(\mathbf{I^{-\!\!*}_{6.3.3}})$
2	$\varphi * (\varphi \mathrel{-\!\!*} \neg(\psi \wedge \chi)) \Rightarrow \neg(\psi \wedge \chi)$	$(\mathbf{I^{-\!\!*}_{6.3.3}})$
3	$(\varphi * (\varphi \mathrel{-\!\!*} \chi)) \wedge (\varphi * (\varphi \mathrel{-\!\!*} \neg(\psi \wedge \chi))) \Rightarrow \neg\psi$	PC, 1, 2
4	$\varphi * ((\varphi \mathrel{-\!\!*} \chi) \wedge (\varphi \mathrel{-\!\!*} \neg(\psi \wedge \chi))) \Rightarrow$ $(\varphi * (\varphi \mathrel{-\!\!*} \chi)) \wedge (\varphi * (\varphi \mathrel{-\!\!*} \neg(\psi \wedge \chi)))$	$*$**-Ilr**, PC
5	$\varphi * ((\varphi \mathrel{-\!\!*} \chi) \wedge (\varphi \mathrel{-\!\!*} \neg(\psi \wedge \chi))) \Rightarrow \neg\psi$	$\Rightarrow$**-Tr**, 4
6	$(\varphi \mathrel{-\!\!*} \chi) \wedge (\varphi \mathrel{-\!\!*} \neg(\psi \wedge \chi)) \Rightarrow (\varphi \mathrel{-\!\!*} \neg\psi)$	$(\mathbf{A^*_7})$, $*$**-Adj**, 5
7	$(\varphi \mathrel{-\!\!*} \chi) \wedge \neg(\varphi \mathrel{-\!\!*} \neg\psi) \Rightarrow \neg(\varphi \mathrel{-\!\!*} \neg(\psi \wedge \chi))$	PC
8	$(\varphi \mathrel{-\!\!*} \chi) \wedge (\varphi \mathrel{-\!\!\circledast} \psi) \Rightarrow (\varphi \mathrel{-\!\!\circledast} \psi \wedge \chi)$	Def. $-\!\!\circledast$, 7 $\square$

Proof of $\mathbf{(I^{-\!*}_{6.3.10})}$ *and* $\mathbf{(I^{-\!*}_{6.3.11})}$. Below, we provide the derivation for the admissible axiom schema $\mathbf{(I^{-\!*}_{6.3.10})}$ (the derivation for $\mathbf{(I^{-\!*}_{6.3.11})}$ is very similar and is thus omitted).

1	$\varphi \Rightarrow (\varphi \wedge \mathtt{x} = \mathtt{y}) \vee (\varphi \wedge \mathtt{x} \neq \mathtt{y})$	PC
2	$(\varphi \mathrel{-\!\circledast} \psi) \Rightarrow ((\varphi \wedge \mathtt{x} = \mathtt{y}) \vee (\varphi \wedge \mathtt{x} \neq \mathtt{y}) \mathrel{-\!\circledast} \psi)$	$\mathbf{(I^{-\!*}_{6.3.4})}$, 1
3	$(\varphi \mathrel{-\!\circledast} \psi) \Rightarrow (\varphi \wedge \mathtt{x} = \mathtt{y} \mathrel{-\!\circledast} \psi) \vee (\varphi \wedge \mathtt{x} \neq \mathtt{y} \mathrel{-\!\circledast} \psi)$	$\mathbf{(I^{-\!*}_{6.3.7})}$, $\Rightarrow$**-Tr**, 2
4	$\mathtt{x} = \mathtt{y} * \mathtt{x} \neq \mathtt{y} \Rightarrow \mathtt{x} = \mathtt{y}$	$\mathbf{(A^{*}_{14})}$, $*$**-Ilr**
5	$\mathtt{x} \neq \mathtt{y} * \mathtt{x} = \mathtt{y} \Rightarrow \mathtt{x} \neq \mathtt{y}$	$\mathbf{(A^{*}_{14})}$, $*$**-Ilr**
6	$\mathtt{x} = \mathtt{y} * \mathtt{x} \neq \mathtt{y} \Rightarrow \mathtt{x} = \mathtt{y} \wedge \mathtt{x} \neq \mathtt{y}$	$\mathbf{(A^{*}_{7})}$, $\Rightarrow$**-Tr**, PC, 4, 5
7	$\mathtt{x} = \mathtt{y} * \mathtt{x} \neq \mathtt{y} \Rightarrow \neg\top$	PC, 6
8	$\neg\top \Rightarrow \neg\psi$	PC
9	$\mathtt{x} = \mathtt{y} * \mathtt{x} \neq \mathtt{y} \Rightarrow \neg\psi$	PC, 7, 8
10	$\mathtt{x} = \mathtt{y} \Rightarrow (\mathtt{x} \neq \mathtt{y} \mathrel{-\!*} \neg\psi)$	$*$**-Adj**, 9
11	$\neg(\mathtt{x} \neq \mathtt{y} \mathrel{-\!*} \neg\psi) \Rightarrow \mathtt{x} \neq \mathtt{y}$	PC, 10
12	$(\mathtt{x} \neq \mathtt{y} \mathrel{-\!\circledast} \psi) \Rightarrow \mathtt{x} \neq \mathtt{y}$	Def. $-\!\circledast$, 11
13	$\varphi \wedge \mathtt{x} \neq \mathtt{y} \Rightarrow \mathtt{x} \neq \mathtt{y}$	PC
14	$(\varphi \wedge \mathtt{x} \neq \mathtt{y} \mathrel{-\!\circledast} \psi) \Rightarrow (\mathtt{x} \neq \mathtt{y} \mathrel{-\!\circledast} \psi)$	$\mathbf{(I^{-\!*}_{6.3.4})}$, 13
15	$(\varphi \wedge \mathtt{x} \neq \mathtt{y} \mathrel{-\!\circledast} \psi) \Rightarrow \mathtt{x} \neq \mathtt{y}$	$\Rightarrow$**-Tr**, 12, 14
16	$\mathtt{x} = \mathtt{y} \wedge (\varphi \mathrel{-\!\circledast} \psi) \Rightarrow (\varphi \wedge \mathtt{x} = \mathtt{y} \mathrel{-\!\circledast} \psi) \vee \mathtt{x} \neq \mathtt{y}$	PC, 3, 15
17	$\mathtt{x} = \mathtt{y} \wedge (\varphi \mathrel{-\!\circledast} \psi) \Rightarrow (\varphi \wedge \mathtt{x} = \mathtt{y} \mathrel{-\!\circledast} \psi)$	PC, 16 $\square$

Proof of $\mathbf{(I^{-\!*}_{6.3.12})}$. Notice that, since $\varphi_{\mathtt{size}}$ is satisfiable, for every $\beta_1, \beta_2 \in \mathbb{N}$ such that $\mathtt{size} \geqslant \beta_1 \wedge \neg\mathtt{size} \geqslant \beta_2 \subseteq_{\mathtt{Lt}} \varphi_{\mathtt{size}}$, we must have $\beta_1 < \beta_2$. Moreover, thanks to $\mathbf{(I^{\mathsf{C}}_{5})}$ and $\mathbf{(I^{-\!*}_{6.3.4})}$, without loss of generality, we can restrict ourselves to $\varphi_{\mathtt{size}}$ of the form:
(1) $\varphi_{\mathtt{size}} = \mathtt{size} \geqslant \beta$ for some $\beta \geqslant 0$,
(2) $\varphi_{\mathtt{size}} = \neg(\mathtt{size} \geqslant \beta)$ for some $\beta > 0$,
(3) $\varphi_{\mathtt{size}} = \mathtt{size} \geqslant \beta_1 \wedge \neg(\mathtt{size} \geqslant \beta_2)$ for some $\beta_2 > \beta_1$.
Indeed, given an arbitrary $\varphi_{\mathtt{size}}$, every positive literal $\mathtt{size} \geqslant \beta$ such that $\beta < \max_{\mathtt{size}}(\varphi_{\mathtt{size}})$ can be derived starting from $\mathtt{size} \geqslant \max_{\mathtt{size}}(\varphi_{\mathtt{size}})$, by repeated applications of $\mathbf{(I^{\mathsf{C}}_{5})}$. Similarly, let $\overline{\beta}$ be the smallest natural number such that $\neg\mathtt{size} \geqslant \overline{\beta} \subseteq_{\mathtt{Lt}} \varphi_{\mathtt{size}}$, if any. Every literal $\neg\mathtt{size} \geqslant \beta' \subseteq_{\mathtt{Lt}} \varphi_{\mathtt{size}}$ with $\beta' \geqslant \overline{\beta}$ can be derived from $\neg\mathtt{size} \geqslant \overline{\beta}$, by repeated applications of the axiom $\mathbf{(I^{\mathsf{C}}_{5})}$ (taken in contrapositive form i.e. $\neg\mathtt{size} \geqslant \beta \Rightarrow \neg\mathtt{size} \geqslant \beta{+}1$, which is derivable in $\mathcal{H}_{\mathsf{C}}$ by propositional reasoning).

We write $\mathsf{U}(\mathtt{X})$ to denote the conjunction $\bigwedge_{\mathtt{x}\in\mathtt{X}} \neg\mathtt{alloc}(\mathtt{x})$ ('U' stands for 'unallocated'). Below, given $\beta \in \mathbb{N}$, we aim at deriving the formula $(\mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X})) \mathrel{-\!\circledast} \top$ since this implies that $\mathbf{(I^{-\!*}_{6.3.12})}$ is derivable in its instances (1)–(3), as shown below.
case (1): Let $\varphi_{\mathtt{size}} = \mathtt{size} \geqslant \beta$.

1	$\mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\circledast} \top$	Hypothesis

2	$\mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X}) \Rightarrow \mathtt{size} \geqslant \beta \wedge \mathsf{U}(\mathtt{X})$	PC, def. of $\mathtt{size} = \beta$
3	$(\mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top) \Rightarrow (\mathtt{size} \geqslant \beta \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top)$	$(\mathbf{I}^{-\!*}_{\mathbf{6.3.4}})$, 2
4	$\mathtt{size} \geqslant \beta \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top$	Modus Ponens, 1, 3

case (2): Let $\varphi_{\mathtt{size}} = \neg\mathtt{size} \geqslant \beta$. Since $\varphi_{\mathtt{size}}$ is satisfiable, we have $\beta \geqslant 1$.

1	$\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top$	Hypothesis
2	$\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X}) \Rightarrow \neg\mathtt{size} \geqslant \beta \wedge \mathsf{U}(\mathtt{X})$	PC, def. of $\mathtt{size} = \beta{-}1$
3	$(\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top) \Rightarrow (\neg\mathtt{size} \geqslant \beta \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top)$	$(\mathbf{I}^{-\!*}_{\mathbf{6.3.4}})$, 2
4	$\neg\mathtt{size} \geqslant \beta \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top$	Modus Ponens, 1, 3

case (3): Let $\varphi_{\mathtt{size}} = \mathtt{size} \geqslant \beta_1 \wedge \neg\mathtt{size} \geqslant \beta_2$. Since $\varphi_{\mathtt{size}}$ is satisfiable, $\beta_2 > \beta_1$.

1	$\mathtt{size} = \beta_2{-}1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top$	Hypothesis
2	$\mathtt{size} = \beta_2{-}1 \Rightarrow \mathtt{size} \geqslant \beta_1$	repeated $(\mathbf{I}^{\mathsf{C}}_{\mathbf{5}})$, as $\beta_2 > \beta_1$
3	$\mathtt{size} = \beta_2{-}1 \Rightarrow \neg\mathtt{size} \geqslant \beta_2$	PC, def. of $\mathtt{size} = \beta{-}1$
4	$\mathtt{size} = \beta_2{-}1 \wedge \mathsf{U}(\mathtt{X}) \Rightarrow \mathtt{size} \geqslant \beta_1 \wedge \neg\mathtt{size} \geqslant \beta_2 \wedge \mathsf{U}(\mathtt{X})$	PC, 2, 3
5	$\big(\mathtt{size} = \beta_2{-}1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top\big) \Rightarrow$ $(\mathtt{size} \geqslant \beta_1 \wedge \neg\mathtt{size} \geqslant \beta_2 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top)$	$(\mathbf{I}^{-\!*}_{\mathbf{6.3.4}})$, 4
6	$\mathtt{size} \geqslant \beta_1 \wedge \neg\mathtt{size} \geqslant \beta_2 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top$	Modus Ponens, 1, 5

To conclude the proof, let us show that $(\mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X})) \mathrel{-\!\!\circledast} \top$ is derivable in $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$. The proof is by induction on β, with two base cases, for $\beta = 0$ and $\beta = 1$.

base case: $\beta = 0$**:** In this case, $\mathtt{size} = 0$ is equal to $\mathtt{size} \geqslant 0 \wedge \neg\mathtt{size} \geqslant 1$. We have,

1	$(\mathtt{emp} -\!\!* \bot) \Rightarrow \mathtt{emp} * (\mathtt{emp} -\!\!* \bot)$	$(\mathbf{A}^{*}_{\mathbf{11}})$
2	$\mathtt{emp} * (\mathtt{emp} -\!\!* \bot) \Rightarrow \bot$	$(\mathbf{I}^{-\!*}_{\mathbf{6.3.3}})$
3	$(\mathtt{emp} -\!\!* \bot) \Rightarrow \bot$	$\Rightarrow$**-Tr**, 1, 2
4	$\mathtt{emp} \mathrel{-\!\!\circledast} \top$	PC, 3, def. of $-\!\!\circledast$
5	$\mathtt{alloc}(\mathtt{x}) \Rightarrow \mathtt{size} \geqslant 1$	$(\mathbf{I}^{\mathsf{C}}_{\mathbf{6}})$
6	$\mathtt{emp} \Rightarrow \neg\mathtt{alloc}(\mathtt{x})$	PC, 5, as $\mathtt{size} \geqslant 1 = \neg\mathtt{emp}$
7	$\mathtt{emp} \Rightarrow \mathsf{U}(\mathtt{X})$	PC, 6 used for all $\mathtt{x} \in \mathtt{X}$
8	$\mathtt{emp} \Rightarrow \mathtt{size} \geqslant 0 \wedge \neg(\mathtt{size} \geqslant 1)$	PC, def. of $\mathtt{size} \geqslant \beta$
9	$\mathtt{emp} \Rightarrow \mathtt{size} \geqslant 0 \wedge \neg(\mathtt{size} \geqslant 1) \wedge \mathsf{U}(\mathtt{X})$	PC, 7, 8
10	$(\mathtt{emp} \mathrel{-\!\!\circledast} \top) \Rightarrow (\mathtt{size} \geqslant 0 \wedge \neg(\mathtt{size} \geqslant 1) \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top)$	$(\mathbf{I}^{-\!*}_{\mathbf{6.3.4}})$, 9
11	$\mathtt{size} \geqslant 0 \wedge \neg(\mathtt{size} \geqslant 1) \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top$	Modus Ponens, 4, 10

base case: $\beta = 1$**:** This case corresponds exactly to the axiom $(\mathbf{A}^{-\!*}_{\mathbf{21}})$.

induction step: $\beta \geqslant 2$**:** First of all, we notice that the following formula is valid:

$$(\mathtt{size} = 1 \wedge \mathsf{U}(\mathtt{X})) * (\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X})) \Rightarrow \mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X}). \qquad (\dagger)$$

Indeed, let (s, h) be a memory state satisfying the antecedent of the implication above. So, there are disjoint heaps h_1 and h_2 such that $h = h_1{+}h_2$, $\mathrm{card}(\mathrm{dom}(h_1)) = 1$, $\mathrm{card}(\mathrm{dom}(h_2)) = \beta - 1$, and for every $\mathtt{x} \in \mathtt{X}$, $s(\mathtt{x}) \notin \mathrm{dom}(h_1)$ and $s(\mathtt{x}) \notin \mathrm{dom}(h_2)$. By $h = h_1{+}h_2$, $\mathrm{card}(\mathrm{dom}(h)) = \mathrm{card}(\mathrm{dom}(h_1)) + \mathrm{card}(\mathrm{dom}(h_2)) = \beta$, and for every $\mathtt{x} \in \mathtt{X}$, $s(\mathtt{x}) \notin \mathrm{dom}(h)$. Thus, $(s, h) \models \mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X})$.

As (†) can be seen as a formula in $\mathsf{SL}(*, \mathtt{alloc})$, by Theorem 5.6 it is derivable in $\mathcal{H}_{\mathsf{C}}(*)$ and thus in $\mathcal{H}_{\mathsf{C}}(*, -\!\!*)$. Now, let us derive $(\mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X})) \mathrel{-\!\!\circledast} \top$. Let us consider as induction hypothesis the derivability of $(\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X})) \mathrel{-\!\!\circledast} \top$. Therefore,

1	$\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top$	Induction Hypothesis
2	$(\mathtt{size} = 1 \wedge \mathsf{U}(\mathtt{X})) * (\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X})) \Rightarrow \mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X})$	(†), see above
3	$\mathtt{size} = 1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top$	$\mathbf{(A^{-\!*}_{21})}$
4	$\top \Rightarrow (\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top)$	PC, 1
5	$(\mathtt{size} = 1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top) \Rightarrow$ $\big(\mathtt{size} = 1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} (\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top)\big)$	$\mathbf{(I^{-\!*}_{6.3.5})}$, 4
6	$\big(\mathtt{size} = 1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} (\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top)\big) \Rightarrow$ $\big((\mathtt{size} = 1 \wedge \mathsf{U}(\mathtt{X})) * (\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X})) \mathrel{-\!\!\circledast} \top\big)$	$\mathbf{(I^{-\!*}_{6.3.6})}$
7	$\big((\mathtt{size} = 1 \wedge \mathsf{U}(\mathtt{X})) * (\mathtt{size} = \beta{-}1 \wedge \mathsf{U}(\mathtt{X})) \mathrel{-\!\!\circledast} \top\big) \Rightarrow$ $(\mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top)$	$\mathbf{(I^{-\!*}_{6.3.4})}$, 2
8	$(\mathtt{size} = 1 \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top) \Rightarrow (\mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top)$	$\Rightarrow$**-Tr**, 5, 6, 7
9	$\mathtt{size} = \beta \wedge \mathsf{U}(\mathtt{X}) \mathrel{-\!\!\circledast} \top$	Modus Ponens, 3, 8 $\square$