On the Expressive Completeness of Bernays-Schönfinkel-Ramsey Separation Logic

Mnacho Echenim[1], Radu Iosif[2] and Nicolas Peltier[1]

[1] Univ. Grenoble Alpes, CNRS, LIG, F-38000 Grenoble France
[2] Univ. Grenoble Alpes, CNRS, VERIMAG, F-38000 Grenoble France

Abstract. This paper investigates the satisfiability problem for Separation Logic, with unrestricted nesting of separating conjunctions and implications, for prenex formulae with quantifier prefix in the language $\exists^*\forall^*$, in the cases where the universe of possible locations is either countably infinite or finite. In analogy with first-order logic with uninterpreted predicates and equality, we call this fragment Bernays-Schönfinkel-Ramsey Separation Logic [$\mathsf{BSR}(\mathsf{SL}^k)$]. We show that, unlike in first-order logic, the (in)finite satisfiability problem is undecidable for $\mathsf{BSR}(\mathsf{SL}^k)$ and we define two non-trivial subsets thereof, that are decidable for finite and infinite satisfiability, respectively, by controlling the occurrences of universally quantified variables within the scope of separating implications, as well as the polarity of the occurrences of the latter. The decidability results are obtained by a controlled elimination of separating connectives, described as (i) an effective translation of a prenex form Separation Logic formula into a combination of a small number of *test formulae*, using only first-order connectives, followed by (ii) a translation of the latter into an equisatisfiable first-order formula.

1 Introduction

Separation Logic [9,14] is a logical framework used in program verification to describe properties of the dynamically allocated memory, such as topologies of data structures (lists, trees), (un)reachability between pointers, etc. The quest for automated push-button program verification methods motivates the need for understanding the decidability, complexity and expressive power of various dialects thereof, that are used as assertion languages in Hoare-style proofs [9], or logic-based abstract domains in static analysis [4].

In a nutshell, given an integer $k \geq 1$, the logic SL^k is obtained from the first-order theory of a finite functional relation of arity $k+1$, called a *heap*[3], by adding two non-classical connectives: (i) the *separating conjunction* $\phi_1 * \phi_2$, that asserts a split of the heap into disjoint heaps satisfying ϕ_1 and ϕ_2 respectively, and (ii) the *separating implication* or *magic wand* $\phi_1 \mathrel{-\!\!*} \phi_2$, stating that each extension of the heap by a heap satisfying ϕ_1 must satisfy ϕ_2. The separating

[3] Intuitively, k is the number of record fields in each memory cell.

connectives $*$ and $\multimap$ allow concise definitions of program semantics, via weakest precondition calculi [9] and easy-to-write specifications of recursive linked data structures (e.g. singly- and doubly-linked lists, trees with linked leaves and parent pointers, etc.), when higher-order inductive definitions are added [14].

A typical problem in verification, occurring as a subgoal in a Hoare-style proof of a program or in an inductive proof of inclusion between least fixed point models (sets of heaps) of higher-order predicates, is deciding the validity of entailments between existentially quantified formulae in the base assertion language. This problem is reduced to the (un)satisfiability of an SL^k formula with quantifier prefix in the language $\exists^*\forall^*$. In analogy with first-order logic with equality and uninterpreted predicates [11], we call this fragment Bernays-Schönfinkel-Ramsey Separation Logic [$\mathsf{BSR}(\mathsf{SL}^k)$].

Unlike the Bernays-Schönfinkel-Ramsey fragment of first-order logic, $\mathsf{BSR}(\mathsf{SL}^k)$ is difficult to reason about, due to the unrestricted use of separating connectives. A way to circumvent this problem is to define a small set of patterns, called *test formulae* in the literature [**?**,3,7,8], that are parametric in their arguments and some integer constants, and prove that every formula in the fragment is equivalent to a classical combination of instances of those patterns, bound only with first-order connectives.

These expressive completeness results are, in some sense, similar to the elimination of existential quantifiers in some interpreted theories of first-order logic, such as Presburger arithmetic. In fact, the existential quantifiers are not completely eliminated, but rather confined to a small set of modulo constraints, in which they occur in a controlled fashion. Similarly, in SL^k, it is possible to confine the separating conjunction $*$ and implication $\multimap$ to a small set of test formulae and convert each SL^k formula from a certain fragment into an equivalent boolean combination of test formulae. As with Presburger arithmetic, this is an argument for showing decidability of the logical fragment under consideration.

Our contributions The main contributions of this paper are:

1. We show that the finite and infinite satisfiability problems are undecidable for the logic $\mathsf{BSR}(\mathsf{SL}^k)$, interpreted over heaps with $k \geq 2$ record fields. The main reason for undecidability lies in the presence of universally quantified variables within the scope of a separating implication, that occurs, moreover, under an even number of negations.
2. By disallowing universally quantified variables in the scope of positive occurrences of separating implications, and even stronger, disallowing positive occurrences thereof, we define two non-trivial fragments $\mathsf{BSR}^{\mathit{inf}}(\mathsf{SL}^k)$ and $\mathsf{BSR}^{\mathit{fin}}(\mathsf{SL}^k)$ of $\mathsf{BSR}(\mathsf{SL}^k)$, for which the infinite and finite satisfiability problems are PSPACE-complete, respectively. These results establish neat decidability frontiers within $\mathsf{BSR}(\mathsf{SL}^k)$.

In contrast with the majority of the literature on Separation Logic, here the universe of *available* memory locations (besides the ones occurring in the heap, which is finite) is not automatically assumed to be infinite. In fact, we consider both cases in which the universe is countably infinite and finite. In particular, the finite universe hypothesis is useful when dealing with bounded memory issues, for instance checking that the execution of the program satisfies its postcondition, provided that there are enough many available memory cells.

Having different interpretations of the universe is also motivated by a recent integration of SL^k within a DPLL(T)-based SMT solver [13,12], in which the SL theory is parameterized by the theory of locations, just like the theories of arrays and sets are parameterized by theories of values.

Surprisingly, when considering a finite universe, the separating connectives allow to define bounds also on the cardinality of the universe and on the number of free locations (not in the heap), besides specifying the shape and cardinality of the heap. As a result, the conditions needed for decidability within $\mathsf{BSR}(\mathsf{SL}^k)$ turn out to be stronger for finite universes than for infinite ones. The argument for decidability relies on (i) the definition of a restricted set of test formulae capturing all properties of heaps, that can be expressed in quantifier-free SL^k, together with (ii) an equivalence-preserving syntactic translation of a prenex form SL^k formula into a boolean combination of test formulae, with the same quantifier prefix. The latter formula is translated into first-order logic and decidability is established by tracking those formulae of $\mathsf{BSR}(\mathsf{SL}^k)$ that translate into the classical Bernays-Schönfinkel-Ramsey fragment of first-order logic [11].

Related Work. Expressive completeness results exist for quantifier-free SL^1 [**?**,3] and for SL^1 with one and two quantified variables [8,7]. There, the existence of equivalent boolean combinations of test formulae is showed implicitly, using a finite enumeration of equivalence classes of models, instead of an effective transformation. Instead, here we present an explicit equivalence-preserving transformation of quantifier-free SL^k formulae over heaps with $k \geq 2$ record fields into boolean combinations of test formulae, and translate the latter into first-order logic.

Another translation of quantifier-free SL^k into first-order logic with equality has been described in [5]. There, the small model property of quantifier-free SL^k [6] is used to bound the number of first-order variables to be considered and the separating connectives are interpreted as first-order quantifiers. The result is an equisatisfiable first-order formula whose satisfiability can be checked in PSPACE. This translation scheme cannot be, however, directly applied to $\mathsf{BSR}(\mathsf{SL}^k)$, which does not have a small model property, and is, moreover, undecidable.

Existing decidability and complexity results for various SL^k fragments [6,3,8,7] always assume the universe of heap locations to be countably infinite. In this paper we consider, in addition, the case where the universe is finite. Theory-parameterized versions of $\mathsf{BSR}(\mathsf{SL}^k)$ have been shown to be undecidable, e.g. when integer linear arithmetic is used to reason about locations, and wrongly claimed to be PSPACE-complete for countably infinite and finite unbounded location sorts, with no relation other than equality [12]. Here we correct the wrong claim of [12] and draw a precise chart of decidability for both infinite and finite satisfiability of $\mathsf{BSR}(\mathsf{SL}^k)$.

2 Preliminaries

We denote by $\mathbb{Z}$ the set of integers and by $\mathbb{N}$ the set of positive integers including zero. We define $\mathbb{Z}_\infty = \mathbb{Z} \cup \{\infty\}$ and $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$, where for each $n \in \mathbb{Z}$ we have $n + \infty = \infty$ and $n < \infty$. For a countable set S we denote by $\|S\| \in \mathbb{N}_\infty$ the cardinality of S. A decision problem is in $(\mathsf{N})\mathsf{SPACE}(n)$ if it can be decided by a (nondeterministic) Turing machine in space $O(n)$ and in PSPACE if it is in $\mathsf{SPACE}(n^c)$ for some integer $c \geq 1$, independent of the input.

Let Var be a countable set of variables, denoted as x, y, z and U be a sort. A *function symbol* f has $\#(f) \geq 0$ arguments of sort U and a sort $\sigma(f)$, which is either the boolean sort Bool or U. If $\#(f) = 0$, we call f a *constant*. We use $\bot$ and $\top$ for the boolean constants false and true, respectively. First-order (FO) terms t and formulae φ are defined by the following grammar:

$$t := x \mid f(t_1, \ldots, t_{\#(f)})$$
$$\varphi := \bot \mid \top \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi_1 \mid \exists x \,.\, \varphi_1 \mid t_1 \approx t_2 \mid p(t_1, \ldots, t_{\#(p)})$$

where $x \in \mathsf{Var}$, f and p are function symbols, $\sigma(f) = U$ and $\sigma(p) = \mathsf{Bool}$. We write $\varphi_1 \vee \varphi_2$ for $\neg(\neg\varphi_1 \wedge \neg\varphi_2)$, $\varphi_1 \rightarrow \varphi_2$ for $\neg\varphi_1 \vee \varphi_2$, $\varphi_1 \leftrightarrow \varphi_2$ for $\varphi_1 \rightarrow \varphi_2 \wedge \varphi_2 \rightarrow \varphi_1$ and $\forall x \,.\, \varphi$ for $\neg\exists x \,.\, \neg\varphi$.

The size of a formula φ, denoted as $\mathsf{size}(\varphi)$, is the number of symbols needed to write it down. Let $\mathsf{var}(\varphi)$ be the set of variables that occur free in φ, i.e. not in the scope of a quantifier. A *sentence* φ is a formula where $\mathsf{var}(\varphi) = \emptyset$. Given formulae φ, ϕ and ψ, we write $\varphi[\phi]$ when ϕ is a subformula of φ and denote by $\varphi[\psi/\phi]$ the formula obtained by substituting ψ for ϕ in φ.

First-order formulae are interpreted over FO-structures (called structures, when no confusion arises) $\mathcal{S} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$, where $\mathfrak{U}$ is a countable set, called the *universe*, the elements of which are called *locations*, $\mathfrak{s} : \mathsf{Var} \rightharpoonup \mathfrak{U}$ is a mapping of variables to locations, called a *store* and $\mathfrak{i}$ interprets each function symbol f by a function $f^{\mathfrak{i}} : \mathfrak{U}^{\#(f)} \to \mathfrak{U}$, if $\sigma(f) = U$ and $f^{\mathfrak{i}} : \mathfrak{U}^{\#(f)} \to \{\bot^{\mathfrak{i}}, \top^{\mathfrak{i}}\}$ if $\sigma(f) = \mathsf{Bool}$. A structure $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$ is *finite* when $\|\mathfrak{U}\| \in \mathbb{N}$ and *infinite* otherwise.

We write $\mathcal{S} \models \varphi$ iff φ is true when interpreted in $\mathcal{S}$. This relation is defined recursively on the structure of φ, as usual. When $\mathcal{S} \models \varphi$, we say that $\mathcal{S}$ is a *model* of φ. A formula is *satisfiable* when it has a model. We write $\varphi_1 \models \varphi_2$ when every model of φ_1 is also a model of φ_2 and by $\varphi_1 \equiv \varphi_2$ we mean $\varphi_1 \models \varphi_2$ and $\varphi_1 \models \varphi_2$. The *(in)finite satisfiability problem* asks, given a formula φ, whether a (in)finite model exists for this formula.

The Bernays-Schönfinkel-Ramsey fragment of FO, denoted by $\mathsf{BSR}(\mathsf{FO})$, is the set of sentences $\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_m \,.\, \varphi$, where φ is a quantifier-free formula in which all function symbols f of arity $\#(f) > 0$ have sort $\sigma(f) = \mathsf{Bool}$. It is known that any satisfiable $\mathsf{BSR}(\mathsf{FO})$ sentence has a finite model with at most $\max(1, n)$ locations, where n is the length of the existential quantifier prefix[4].

2.1 Separation Logic

Let $k \in \mathbb{N}$ be a strictly positive integer. The logic SL^k is the set of formulae generated by the grammar below:

$$\varphi := \bot \mid \top \mid \mathsf{emp} \mid x \approx y \mid x \mapsto (y_1, \ldots, y_k) \mid \\ \varphi \wedge \varphi \mid \neg\varphi \mid \varphi * \varphi \mid \varphi \mathrel{-\!\!*} \varphi \mid \exists x \,.\, \varphi$$

where $x, y, y_1, \ldots, y_k \in \mathsf{Var}$. The connectives $*$ and $\mathrel{-\!\!*}$ are respectively called the *separating conjunction* and *separating implication* (*magic wand*). We write $\varphi_1 \multimap \varphi_2$ for $\neg(\varphi_1 \mathrel{-\!\!*} \neg\varphi_2)$ (also called *septraction*) and denote by $\mathbf{y}$, $\mathbf{y}'$ the tuples $(y_1, \ldots, y_k), (y'_1, \ldots, y'_k) \in \mathsf{Var}^k$, respectively. The size of an SL^k formula φ, denoted $\mathsf{size}(\varphi)$, is the number of symbols needed to write it down.

Given an SL^k formula ϕ and a subformula ψ of ϕ, we say that ψ *occurs at polarity* $p \in \{-1, 0, 1\}$ iff one of the following holds: (i) $\phi = \psi$ and $p = 1$, (ii) $\phi = \neg\phi_1$ and ψ occurs at polarity $-p$ in ϕ_1, (iii) $\phi = \phi_1 \wedge \phi_2$ or $\phi = \phi_1 * \phi_2$, and ψ occurs at polarity p in ϕ_i, for some $i = 1, 2$, or (iv) $\phi = \phi_1 \mathrel{-\!\!*} \phi_2$ and either ψ is a subformula of ϕ_1 and $p = 0$, or ψ occurs at polarity p in ϕ_2. A polarity of $1, 0$ or -1 is also referred to as positive, neutral or negative, respectively.

SL^k formulae are interpreted over SL-*structures* (called structures when no confusion arises) $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$, where $\mathfrak{U}$ and $\mathfrak{s}$ are as before and $\mathfrak{h} : \mathfrak{U} \rightharpoonup_{fin} \mathfrak{U}^k$ is a finite partial mapping of locations to k-tuples of locations, called a *heap*. As before, a structure $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ is finite when $||\mathfrak{U}|| \in \mathbb{N}$ and infinite otherwise. We denote by $\mathrm{dom}(\mathfrak{h})$ the domain of the heap $\mathfrak{h}$ and by $||\mathfrak{h}|| \in \mathbb{N}$ the cardinality of $\mathrm{dom}(\mathfrak{h})$. Two heaps $\mathfrak{h}_1$ and $\mathfrak{h}_2$ are *disjoint* iff $\mathrm{dom}(\mathfrak{h}_1) \cap \mathrm{dom}(\mathfrak{h}_2) = \emptyset$, in which case $\mathfrak{h}_1 \uplus \mathfrak{h}_2$ denotes their union ($\uplus$ is undefined for non-disjoint heaps). A heap

[4] See, e.g., [2, Proposition 6.2.17].

$\mathfrak{h}'$ is an *extension* of $\mathfrak{h}$ iff $\mathfrak{h}' = \mathfrak{h} \uplus \mathfrak{h}''$, for some heap $\mathfrak{h}''$. The relation $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \varphi$ is defined inductively, as follows:

$$
\begin{array}{lcl}
(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{emp} & \Leftrightarrow & \mathfrak{h} = \emptyset \\
(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models x \mapsto (y_1, \ldots, y_k) & \Leftrightarrow & \mathfrak{h} = \{\langle \mathfrak{s}(x), (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))\rangle\} \\
(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \varphi_1 * \varphi_2 & \Leftrightarrow & \text{there exist disjoint heaps} \\
 & & h_1, h_2 \text{ such that } h = h_1 \uplus h_2 \\
 & & \text{and } (\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_i) \models \varphi_i, \text{ for } i = 1, 2 \\
(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \varphi_1 \mathrel{-\!\!*} \varphi_2 & \Leftrightarrow & \text{for all heaps } \mathfrak{h}' \text{ disjoint from } \mathfrak{h} \\
 & & \text{such that } (\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models \varphi_1, \text{ we} \\
 & & \text{have } (\mathfrak{U}, \mathfrak{s}, \mathfrak{h}' \uplus \mathfrak{h}) \models \varphi_2
\end{array}
$$

The semantics of equality, boolean and first-order connectives is the usual one. Satisfiability, entailment and equivalence are defined for SL^k as for FO formulae. The (in)finite satisfiability problem for SL^k asks whether a (in)finite model exists for a given formula. We write $\phi \equiv^{fin} \psi$ [$\phi \equiv^{inf} \psi$] whenever $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi \Leftrightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \psi$ holds for every finite [infinite] structure $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$.

The Bernays-Schönfinkel-Ramsey fragment of SL^k, denoted by $\mathsf{BSR}(\mathsf{SL}^k)$, is the set of sentences $\exists x_1 \ldots \exists x_n \forall y_1 \ldots \forall y_m \,.\, \phi$, where ϕ is a quantifier-free SL^k formula. Since there are no function symbols of arity greater than zero in SL^k, there are no restrictions, other than the form of the quantifier prefix, defining $\mathsf{BSR}(\mathsf{SL}^k)$.

3 Test Formulae for SL^k

We define a small set of SL^k patterns of formulae, possibly parameterized by a positive integer, called *test formulae*. These patterns capture properties related to allocation, points-to relations in the heap and cardinality constraints.

Definition 1. *The following patterns are called* test formulae*:*

$$
\begin{array}{rcl}
x \hookrightarrow \mathbf{y} & \stackrel{\text{def}}{=} & x \mapsto \mathbf{y} * \top \\
\mathsf{alloc}(x) & \stackrel{\text{def}}{=} & x \mapsto \underbrace{(x, \ldots, x)}_{k \text{ times}} \mathrel{-\!\!*} \bot \\
|h| \geq n & \stackrel{\text{def}}{=} & \begin{cases} |h| \geq n-1 * \neg\mathsf{emp}, & \text{if } n > 0 \\ \top, & \text{if } n = 0 \\ \bot, & \text{if } n = \infty \end{cases} \\
|U| \geq n & \stackrel{\text{def}}{=} & \top \multimap |h| \geq n,\ n \in \mathbb{N} \\
|h| \geq |U| - n & \stackrel{\text{def}}{=} & |h| \geq n+1 \mathrel{-\!\!*} \bot, n \in \mathbb{N}
\end{array}
$$

and $x \approx y$, where $x, y \in \mathsf{Var}$, $\mathbf{y} \in \mathsf{Var}^k$ and $n \in \mathbb{N}_\infty$ is a positive integer or ∞. A literal *is either a test formula or its negation.*

The intuitive semantics of test formulae is formally stated below:

Proposition 1. *Given an* SL*-structure* $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$*, we have:*

$$(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models x \hookrightarrow \mathbf{y} \Leftrightarrow \mathfrak{h}(\mathfrak{s}(x)) = (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))$$
$$(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |U| \geq n \Leftrightarrow ||\mathfrak{U}|| \geq n$$
$$(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{alloc}(x) \Leftrightarrow \mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h})$$
$$(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| \geq |U| - n \Leftrightarrow ||\mathfrak{h}|| \geq ||\mathfrak{U}|| - n$$
$$(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| \geq n \Leftrightarrow ||\mathfrak{h}|| \geq n$$

for all variables $x, y_1, \ldots, y_k \in \mathsf{Var}$ *and integers* $n \in \mathbb{N}$*.*

Proof: Let $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ and, given a set of locations $\mathfrak{U}$ and a finite set $L \subseteq \mathfrak{U}$, we will denote by $\mathfrak{h}_L$ the heap with domain L, such that for all $\ell \in L$, $\mathfrak{h}_L(\ell) = (\ell, \ldots, \ell)$. It is clear that $||\mathfrak{h}_L|| = ||L||$.

$\boxed{\mathcal{I} \models x \hookrightarrow \mathbf{y} \Leftrightarrow \mathfrak{h}(\mathfrak{s}(x)) = (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))}$ Assume that $\mathcal{I} \models x \hookrightarrow \mathbf{y}$. Then by definition, there exist disjoint heaps $\mathfrak{h}_1$, $\mathfrak{h}_2$ such that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models x \mapsto \mathbf{y}$, $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_2) \models \top$ and $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$. Thus $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h}_1) \subseteq \mathrm{dom}(\mathfrak{h})$ and $\mathfrak{h}(\mathfrak{s}(x)) = \mathfrak{h}_1(\mathfrak{s}(x)) = (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))$. Conversely, assume $\mathfrak{h}(\mathfrak{s}(x)) = (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))$. Then $\mathfrak{h}$ is of the form $\mathfrak{h}_1 \uplus \mathfrak{h}_2$, where $\mathfrak{h}_1$ is the restriction of $\mathfrak{h}$ to $\{\mathfrak{s}(x)\}$ and $\mathfrak{h}_2$ is the restriction of $\mathfrak{h}$ to $\mathfrak{U} \setminus \{\mathfrak{s}(x)\}$. It is straightforward to verify that $\mathfrak{h}_1 \models x \mapsto \mathbf{y}$ and $\mathfrak{h}_2 \models \top$.

$\boxed{\mathcal{I} \models \mathsf{alloc}(x) \Leftrightarrow \mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h})}$ Assume that $\mathcal{I} \models \mathsf{alloc}(x)$. Then there cannot be any heap $\mathfrak{h}_1$ disjoint from $\mathfrak{h}$, such that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models x \mapsto (x, \ldots, x)$. But for $L = \{\mathfrak{s}(x)\}$, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_L) \models x \mapsto (x, \ldots, x)$, thus $\mathfrak{h}_L$ is not disjoint from $\mathfrak{h}$ and necessarily, $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h})$. Conversely, assume $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h})$, and let $\mathfrak{h}_1$ be a heap such that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models x \mapsto (x, \ldots, x)$. Then $\mathfrak{h}_1$ cannot be disjoint from $\mathfrak{h}$, which proves that $\mathcal{I} \models \mathsf{alloc}(x)$.

$\boxed{\mathcal{I} \models |h| \geq n \Leftrightarrow ||\mathfrak{h}|| \geq n}$ Assume that $\mathcal{I} \models |h| \geq n$. Then since $\mathfrak{h}$ has a finite domain, it is clear that $||\mathfrak{h}|| \geq n$ if $n < 0$ and that no such structure exists if $n = \infty$. When $n \geq 0$, we prove the result by induction on n. The case where $n = 0$ is straightforward to prove. Otherwise, there exist disjoint heaps $\mathfrak{h}_1, \mathfrak{h}_2$ such that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models |h| \geq n - 1$, $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_2) \models \neg\mathsf{emp}$ and $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$. By the induction hypothesis $||\mathfrak{h}_1|| \geq n - 1$ and by definition, $||\mathfrak{h}_2|| \geq 1$, so that $||\mathfrak{h}_1 \uplus \mathfrak{h}_2|| \geq n$. Conversely, assume that $||\mathfrak{h}|| \geq n$. This always holds if $n \leq 0$ and never holds if $n = \infty$. Otherwise, we prove the result by induction on n. Assume $n > 0$, so that $\mathrm{dom}(\mathfrak{h}) \neq \emptyset$. Consider $\ell \in \mathrm{dom}(\mathfrak{h})$ and let $\mathfrak{h}_1$ and $\mathfrak{h}_2$ respectively denote the restrictions of $\mathfrak{h}$ to $\mathfrak{U} \setminus \{\ell\}$ and to $\{\ell\}$, so that $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$. Since $||\mathfrak{h}_1|| \geq n - 1$, by the induction hypothesis $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models |h| \geq n - 1$, and since $\mathrm{dom}(\mathfrak{h}_2) \neq \emptyset$, we have the result.

$\boxed{\mathcal{I} \models |U| \geq n \Leftrightarrow ||\mathfrak{U}|| \geq n}$ Assume that $\mathcal{I} \models |U| \geq n$. Then there exists a heap $\mathfrak{h}_1$ disjoint from $\mathfrak{h}$ such that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus \mathfrak{h}_1) \models |h| \geq n$. This entails that $||\mathfrak{h} \uplus \mathfrak{h}_1|| \geq n$

and since $\mathrm{dom}(\mathfrak{h} \uplus \mathfrak{h}_1) \subseteq \mathfrak{U}$, necessarily, $||\mathfrak{U}|| \geq n$. Conversely, if $||\mathfrak{U}|| \geq n$, then there exists a set $L \subseteq \mathfrak{U}$ such that $\mathrm{dom}(\mathfrak{h}) \subseteq L$ and $||L|| = \max\{n, ||\mathfrak{h}||\}$. Then $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus \mathfrak{h}_L) \models |h| \geq n$, which proves that $\mathcal{I} \models |U| \geq n$.

$\boxed{\mathcal{I} \models |h| \geq |U| - n \Leftrightarrow ||\mathfrak{h}|| \geq ||\mathfrak{U}|| - n}$ Assume that $\mathcal{I} \models |h| \geq |U| - n$. Then there is no heap disjoint from $\mathfrak{h}$ with a domain of cardinality at least $n+1$. In particular, if $L = \mathfrak{U} \setminus \mathrm{dom}(\mathfrak{h})$, then necessarily, $||\mathfrak{h}_1|| \leq n$. Since $||\mathfrak{U}|| = ||\mathfrak{h}|| + ||\mathfrak{h}_1||$, we deduce that $||\mathfrak{h}|| \geq ||\mathfrak{U}|| - n$. Conversely, if $||\mathfrak{h}|| \geq ||\mathfrak{U}|| - n$ then there is no heap disjoint from $\mathfrak{h}$ with a domain of cardinality at least $n+1$, so that $\mathcal{I} \models |h| \geq |U| - n$. □

Not all atoms of SL^k are test formulae, for instance $x \mapsto \mathbf{y}$ and emp are not test formulae. However, by Proposition 1, we have the equivalences $x \mapsto \mathbf{y} \equiv x \hookrightarrow \mathbf{y} \wedge \neg|h| \geq 2$ and $\mathsf{emp} \equiv \neg|h| \geq 1$. Moreover, for any $n \in \mathbb{N}$, the test formulae $|U| \geq n$ and $|h| \geq |U| - n$ become trivially true and false, respectively, if we consider the universe to be infinite.

The integer parameter n occurring in $|h| \geq n$, $|U| \geq n$ and $|h| \geq |U| - n$ is assumed to be written in unary notation. We write $t < u$ for $\neg(t \geq u)$ and $t \approx u$ for $t \geq u \wedge t < u + 1$, where $t, u \in \{n, |h|, |U|, |U| - n \mid n \in \mathbb{N}\}$. For technical convenience, we also define the following linear combinations.

Definition 2. *Given integers $\alpha, \beta \in \mathbb{Z}$, where $\alpha \notin \{0, 1\}$, let* $|h| \geq \alpha \cdot |U| + \beta \stackrel{\text{def}}{=}$

$$\begin{cases} \bot & \text{if } \alpha > 1,\ \beta > 0 \\ \top & \text{if } \alpha, \beta < 0 \\ |U| < \left\lceil \frac{1-\beta}{\alpha-1} \right\rceil \wedge \\ \bigwedge_{1 \leq n \leq \left\lfloor \frac{-\beta}{\alpha-1} \right\rfloor} (|U| \approx n \rightarrow |h| \geq \alpha \cdot n + \beta) & \text{if } \alpha > 1,\ \beta \leq 0 \\ \bigwedge_{1 \leq n < \left\lfloor \frac{-\beta}{\alpha} \right\rfloor} (|U| \approx n \rightarrow |h| \geq \alpha \cdot n + \beta) & \text{if } \alpha < 0,\ \beta \geq 0 \end{cases}$$

Proposition 2. *Given an SL-structure $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| \geq \alpha \cdot |U| + \beta$ iff $||\mathfrak{h}|| \geq \alpha \cdot ||\mathfrak{U}|| + \beta$, for all $\alpha, \beta \in \mathbb{Z}$, $\alpha \notin \{0, 1\}$.*

Proof: We distinguish the four cases below:

- If $\alpha > 1$ and $\beta > 0$ then $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \bot \Leftrightarrow ||\mathfrak{U}|| \geq ||\mathfrak{h}|| \geq \alpha \cdot ||\mathfrak{U}|| + \beta$, never.
- If $\alpha < 0$ and $\beta < 0$ then $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \top \Leftrightarrow ||\mathfrak{h}|| \geq 0 \geq \alpha \cdot ||\mathfrak{U}|| + \beta$, always.
- If $\alpha > 1$ and $\beta \geq 0$, assume first that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| \geq \alpha \cdot |U| + \beta$. Then $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |U| < \left\lceil \frac{1-\beta}{\alpha-1} \right\rceil$ thus $1 \leq ||\mathfrak{U}|| < \left\lceil \frac{1-\beta}{\alpha-1} \right\rceil$, by Proposition 1. If $||\mathfrak{U}|| > \left\lfloor \frac{-\beta}{\alpha-1} \right\rfloor$ then $||\mathfrak{U}|| \geq \left\lceil \frac{1-\beta}{\alpha-1} \right\rceil$, which contradicts $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |U| < \left\lceil \frac{1-\beta}{\alpha-1} \right\rceil$, by Proposition 1. Otherwise, we have $||\mathfrak{U}|| = n$, with $1 \leq n \leq \left\lfloor \frac{-\beta}{\alpha-1} \right\rfloor$. In this case $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| \geq \alpha \cdot n + \beta$, which implies $||\mathfrak{h}|| \geq \alpha \cdot ||\mathfrak{U}|| + \beta$, by Proposition 1. Conversely, assume that $||\mathfrak{h}|| \geq \alpha \cdot ||\mathfrak{U}|| + \beta$. Since necessarily $||\mathfrak{U}|| \geq ||\mathfrak{h}||$, we obtain $||\mathfrak{U}|| \geq \alpha \cdot ||\mathfrak{U}|| + \beta$, i.e., $||\mathfrak{U}|| > \alpha \cdot ||\mathfrak{U}|| + \beta - 1$ and thus $||\mathfrak{U}|| < \left\lceil \frac{1-\beta}{\alpha-1} \right\rceil$ hence $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |U| < \left\lceil \frac{1-\beta}{\alpha-1} \right\rceil$. Moreover, if $n = ||U||$ then $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| \geq \alpha \cdot n + \beta$ follows by Proposition 1.

– If $\alpha < 0$ and $\beta \geq 0$, assume first that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| \geq \alpha \cdot |U| + \beta$. If, moreover, $||\mathfrak{U}|| \geq \frac{-\beta}{\alpha}$, then $\alpha \cdot ||\mathfrak{U}|| + \beta \leq 0$, thus $||\mathfrak{h}|| \geq 0 \geq \alpha \cdot ||\mathfrak{U}|| + \beta$ holds. Otherwise, $1 \leq ||\mathfrak{U}|| < \left\lfloor \frac{-\beta}{\alpha} \right\rfloor$ and if $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |U| \approx n$, for some $1 \leq n < \left\lfloor \frac{-\beta}{\alpha} \right\rfloor$, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| \geq \alpha \cdot n + \beta$, thus $||\mathfrak{h}|| \geq \alpha \cdot ||\mathfrak{U}|| + \beta$, by Proposition 1. Conversely, assume that $||\mathfrak{h}|| \geq \alpha \cdot ||\mathfrak{U}|| + \beta$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |U| \approx n$, for some integer $1 \leq n < \left\lfloor \frac{-\beta}{\alpha} \right\rfloor$. By Proposition 1, we have $||\mathfrak{U}|| = n$ and $||\mathfrak{h}|| \geq \alpha \cdot n + \beta$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| \geq \alpha \cdot |U| + \beta$. □

Definition 3. *A variable x is* allocated *in an* SL*-structure $\mathcal{I}$ iff $\mathcal{I} \models \mathsf{alloc}(x)$. For a set of variables $X \subseteq \mathsf{Var}$, let $\mathsf{alloc}(X) \stackrel{\text{def}}{=} \bigwedge_{x \in X} \mathsf{alloc}(x)$ and $\mathsf{nalloc}(X) \stackrel{\text{def}}{=} \bigwedge_{x \in X} \neg\mathsf{alloc}(x)$. For a set T of literals, we define:*

$$\mathsf{av}(T) \stackrel{\text{def}}{=} \{x \in \mathsf{Var} \mid x \approx_T x',\ T \cap \{\mathsf{alloc}(x'), x' \hookrightarrow \mathbf{y} \mid \mathbf{y} \in \mathsf{Var}^k\} \neq \emptyset\}$$

$$\mathsf{nv}(T) \stackrel{\text{def}}{=} \{x \in \mathsf{Var} \mid x \approx_T x',\ \neg\mathsf{alloc}(x') \in T\}$$

$$\mathsf{fp}_X(T) \stackrel{\text{def}}{=} T \cap \{\mathsf{alloc}(x), \neg\mathsf{alloc}(x), x \hookrightarrow \mathbf{y}, \neg x \hookrightarrow \mathbf{y} \mid x \in X, \mathbf{y} \in \mathsf{Var}^k\}$$

We let $\#_a(T) \stackrel{\text{def}}{=} |\mathsf{av}(T)|_T$ be the number of equivalence classes of $\approx_T$ containing variables allocated in every model of T and $\#_n(X, T) \stackrel{\text{def}}{=} |X \cap \mathsf{nv}(T)|_T$ be the number of equivalence classes of $\approx_T$ containing variables from X that are not allocated in any model of T. We also let $\mathsf{fp}_a(T) \stackrel{\text{def}}{=} \mathsf{fp}_{\mathsf{av}(T)}(T)$.

Intuitively, $\mathsf{av}(T)$ [$\mathsf{nv}(T)$] is the set of variables that must be [are never] allocated in every [any] model of T and $\mathsf{fp}_X(T)$ is the *footprint* of T relative to the set $X \subseteq \mathsf{Var}$, i.e. the set of formulae describing allocation and points-to relations over variables from X. For example, if $T = \{x \approx z, \mathsf{alloc}(x), \neg\mathsf{alloc}(y), \neg z \hookrightarrow \mathbf{y}\}$, then $\mathsf{av}(T) = \{x, z\}$, $\mathsf{nv}(T) = \{y\}$, $\mathsf{fp}_a(T) = \{\mathsf{alloc}(x), \neg z \hookrightarrow \mathbf{y}\}$ and $\mathsf{fp}_{\mathsf{nv}(T)}(T) = \{\neg\mathsf{alloc}(y)\}$.

Proposition 3. *Given a set T of test formulae and a structure $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$, if $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{fp}_a(T)$, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models \mathsf{fp}_a(T)$ for any extension $\mathfrak{h}'$ of $\mathfrak{h}$.*

Proof: By a case split on the form of the atom in $\mathsf{fp}_a(T)$, namely $\mathsf{alloc}(x), x \hookrightarrow \mathbf{y}, \neg x \hookrightarrow \mathbf{y}$, with $x \in \mathsf{av}(T)$. For the case $\neg\mathsf{alloc}(x)$, since $x \in \mathsf{av}(T)$ then $\mathsf{alloc}(x') \in T$ for some variable x' such that $x \approx_T x'$, thus $\mathsf{fp}_a(T)$ is unsatisfiable, contradicting the assumption that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{fp}_a(T)$. □

3.1 From Test Formulae to FO

The introduction of test formulae (Definition 1) is motivated by the reduction of the (in)finite satisfiability problem for quantified boolean combinations thereof to the same problem for FO. Given a quantified boolean combination of test formulae ϕ, the FO formula $\tau(\phi)$ is defined by induction on the structure of ϕ:

$$\tau(|h| \geq n) \stackrel{\text{def}}{=} \mathfrak{a}_n \qquad \tau(|U| \geq n) \stackrel{\text{def}}{=} \mathfrak{b}_n$$
$$\tau(|h| \geq |U| - n) \stackrel{\text{def}}{=} \neg\mathfrak{c}_{n+1} \qquad \tau(\neg\phi_1) \stackrel{\text{def}}{=} \neg\tau(\phi_1)$$
$$\tau(x \hookrightarrow \mathbf{y}) \stackrel{\text{def}}{=} \mathfrak{p}(x, y_1, \ldots, y_k)$$
$$\tau(\mathsf{alloc}(x)) \stackrel{\text{def}}{=} \exists y_1 \ldots \exists y_k \;.\; \mathfrak{p}(x, y_1, \ldots, y_k)$$
$$\tau(\phi_1 \wedge \phi_2) \stackrel{\text{def}}{=} \tau(\phi_1) \wedge \tau(\phi_2)$$
$$\tau(\exists x \;.\; \phi_1) \stackrel{\text{def}}{=} \exists x \;.\; \tau(\phi_1)$$

where $\mathfrak{p}$ is a $(k+1)$-ary function symbol of sort Bool and $\mathfrak{a}_n, \mathfrak{b}_n$ and $\mathfrak{c}_n$ are constants of sort Bool, for all $n \in \mathbb{N}$. These function symbols are related by the following axioms, where $\mathfrak{u}_n$, $\mathfrak{v}_n$ and $\mathfrak{w}_n$ are constants of sort U, for all $n > 0$:

$$\forall x \forall \mathbf{y} \forall \mathbf{y}' \;.\; \mathfrak{p}(x, \mathbf{y}) \wedge \mathfrak{p}(x, \mathbf{y}') \rightarrow \bigwedge_{i=1}^{k} y_i \approx y'_i \qquad (P)$$

$$\mathfrak{a}_0 \qquad (A_0)$$
$$\left\{ \begin{array}{l} \exists \mathbf{y} \;.\; \mathfrak{a}_n \rightarrow \mathfrak{a}_{n-1} \wedge \mathfrak{p}(\mathfrak{u}_n, \mathbf{y}) \wedge \bigwedge_{i=1}^{n-1} \neg \mathfrak{u}_i \approx \mathfrak{u}_n \\ \wedge\; \forall x \forall \mathbf{y} \;.\; \neg\mathfrak{a}_n \wedge \mathfrak{p}(x, \mathbf{y}) \rightarrow \bigvee_{i=1}^{n-1} x \approx \mathfrak{u}_i \end{array} \right\} \qquad (A_n)$$
$$\mathfrak{b}_0 \qquad (B_0)$$
$$\left\{ \begin{array}{l} \mathfrak{b}_n \rightarrow \mathfrak{b}_{n-1} \wedge \bigwedge_{i=1}^{n-1} \neg \mathfrak{v}_i \approx \mathfrak{v}_n \\ \wedge\; \forall x \;.\; \neg\mathfrak{b}_n \rightarrow \bigvee_{i=1}^{n-1} x \approx \mathfrak{v}_i \end{array} \right\} \qquad (B_n)$$
$$\mathfrak{c}_0 \qquad (C_0)$$
$$\forall \mathbf{y} \;.\; \mathfrak{c}_n \rightarrow \mathfrak{c}_{n-1} \wedge \neg\mathfrak{p}(\mathfrak{w}_n, \mathbf{y}) \wedge \bigwedge_{i=1}^{n-1} \neg \mathfrak{w}_n \approx \mathfrak{w}_i \qquad (C_n)$$

Intuitively, $\mathfrak{a}_n$ or $\mathfrak{b}_n$ are true iff there are at least n locations in the domain of the heap and in the universe, respectively $\mathfrak{u}_1, \ldots, \mathfrak{u}_n$ and $\mathfrak{v}_1, \ldots, \mathfrak{v}_n$. However, if $\mathfrak{c}_n$ is true, then there are at least n locations $\mathfrak{w}_1, \ldots, \mathfrak{w}_n$ outside of the domain of the heap (free), but the converse does not hold (remark 2). The following remarks motivate some of the restrictions that define decidable fragments of BSR(SL^k), by reduction to BSR(FO) (§5.2).

Remark 1. The translation of alloc(x) introduces existential quantifiers depending on x. For instance, the BSR(SL^k) formula $\phi = \forall x \;.\; \mathsf{alloc}(x)$ is translated as $\tau(\phi) = \forall x \exists y_1 \ldots \exists y_k \;.\; \mathfrak{p}(x, y_1, \ldots, y_k)$, which lies outside of the BSR(FO) fragment. Because upcoming results (Thm. 2) require that $\tau(\phi)$ be in BSR(FO), we consider quantified boolean combinations of test formulae ϕ in which the alloc(x) formulae either occur at a negative polarity, or x is not universally quantified. In both such cases, $\tau(\phi)$ is in BSR(FO) (Lemma 2). ■

Remark 2. The C_n axioms do not state the equivalence of $\mathfrak{c}_n$ with the existence of at least n free locations. Such an equivalence seems to be hard, if not impossible, to express in $\mathsf{BSR}(\mathsf{FO})$[5]. Note that if the domain is infinite then this problem does not arise since the formulae $|h| \geq |U| - n$ are always false. ■

Definition 4. *Given a quantified boolean combination of test formulae ϕ, let $\mathcal{N}(\phi)$ be the maximum integer parameter n occurring in a test formula $\theta \in \{|h| \geq n, |U| \geq n, |h| \geq |U| - n \mid n \in \mathbb{N}\}$ from ϕ and let $\mathcal{A}(\phi) \stackrel{\text{def}}{=} \{P\} \cup \{A_i\}_{i=0}^{\mathcal{N}(\phi)} \cup \{B_i\}_{i=0}^{\mathcal{N}(\phi)} \cup \{C_i\}_{i=0}^{\mathcal{N}(\phi)+1}$ be the set of axioms related to ϕ.*

The relationship between a boolean combination of test formulae ϕ and its translation into FO is stated below.

Lemma 1. *Let ϕ be a quantified boolean combination of test formulae. The following hold, for any universe $\mathfrak{U}$ and any store $\mathfrak{s}$:*

1. *if $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$, for a heap $\mathfrak{h}$, then $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\phi) \wedge \mathcal{A}(\phi)$, for an interpretation $\mathfrak{i}$, and*
2. *if each test formula $|h| \geq |U| - n$ in ϕ occurs at negative polarity and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\phi) \wedge \mathcal{A}(\phi)$, for an interpretation $\mathfrak{i}$, such that $||\mathfrak{p}^{\mathfrak{i}}|| \in \mathbb{N}$, then $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$, for a heap $\mathfrak{h}$.*

Proof: (1) Let $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ be a model of ϕ. Considering an arbitrary interpretation $\bot^{\mathfrak{i}}$ and $\top^{\mathfrak{i}}$ for the boolean constants true and false, we extend $\mathfrak{i}$ to the $(k+1)$-ary function symbol $\mathfrak{p}$, the constants $\mathfrak{a}_i, \mathfrak{b}_i, \mathfrak{c}_j$ of sort Bool and $\mathfrak{u}_i, \mathfrak{v}_i, \mathfrak{w}_i$ of sort U, for all $i \in [0, \mathcal{N}(\phi)]$ and all $j \in [0, \mathcal{N}(\phi) + 1]$, as follows. For all $\ell_0, \ldots, \ell_k \in \mathfrak{U}$ we set $\mathfrak{p}^{\mathfrak{i}}(\ell_0, \ldots, \ell_k) = \top^{\mathfrak{i}}$ if $\mathfrak{h}(\ell_0) = (\ell_1, \ldots, \ell_k)$ and $\mathfrak{p}^{\mathfrak{i}}(\ell_0, \ldots, \ell_k) = \bot^{\mathfrak{i}}$, otherwise. The interpretation of the boolean constants is defined below:

$$\mathfrak{a}_i^{\mathfrak{i}} \stackrel{\text{def}}{=} \begin{cases} \top^{\mathfrak{i}} & \text{if } 0 \leq i \leq \min(||\mathfrak{h}||, \mathcal{N}(\phi)) \\ \bot^{\mathfrak{i}} & \text{if } i > \min(||\mathfrak{h}||, \mathcal{N}(\phi)) \end{cases}$$
$$\mathfrak{b}_i^{\mathfrak{i}} \stackrel{\text{def}}{=} \begin{cases} \top^{\mathfrak{i}} & \text{if } 0 \leq i \leq \min(||\mathfrak{U}||, \mathcal{N}(\phi)) \\ \bot^{\mathfrak{i}} & \text{if } i > \min(||\mathfrak{U}||, \mathcal{N}(\phi)) \end{cases}$$
$$\mathfrak{c}_i^{\mathfrak{i}} \stackrel{\text{def}}{=} \begin{cases} \top^{\mathfrak{i}} & \text{if } 0 \leq i \leq \min(||\mathfrak{U}|| - ||\mathfrak{h}||, \mathcal{N}(\phi) + 1) \\ \bot^{\mathfrak{i}} & \text{if } i > \min(||\mathfrak{U}|| - ||\mathfrak{h}||, \mathcal{N}(\phi) + 1) \end{cases}$$

Finally, the constants of sort U are interpreted as locations, as follows:

- $\mathfrak{u}_1^{\mathfrak{i}}, \ldots, \mathfrak{u}^{\mathfrak{i}}_{\min(||\mathfrak{h}||, \mathcal{N}(\phi))}$ are the first $\min(||\mathfrak{h}||, \mathcal{N}(\phi))$ locations in $\mathrm{dom}(\mathfrak{h})$ and the rest are arbitrary.
- $\mathfrak{v}_1^{\mathfrak{i}}, \ldots, \mathfrak{v}^{\mathfrak{i}}_{\min(||\mathfrak{U}||, \mathcal{N}(\phi))}$ are the first $\min(||\mathfrak{U}||, \mathcal{N}(\phi))$ locations in $\mathfrak{U}$ and the rest are arbitrary.

[5] The converse of C_n: $\forall x \,.\, (\neg \mathfrak{c}_n \wedge \forall \mathbf{y} \,.\, \neg \mathfrak{p}(x, \mathbf{y})) \rightarrow \bigvee_{i=1}^{n-1} x \approx \mathfrak{w}_i$ is not in $\mathsf{BSR}(\mathsf{FO})$.

– $\mathfrak{w}^{\mathfrak{i}}_1, \ldots, \mathfrak{w}^{\mathfrak{i}}_{\min(||\mathfrak{U}||-||\mathfrak{h}||, \mathcal{N}(\phi)+1)}$ are the first $\min(||\mathfrak{U}|| - ||\mathfrak{h}||, \mathcal{N}(\phi) + 1)$ locations in $\mathfrak{U} \setminus \mathrm{dom}(\mathfrak{h})$ and the rest are arbitrary.

Clearly $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \mathcal{A}(\phi)$. We prove $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi \Leftrightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\phi)$ by induction on the structure of ϕ:

– $\phi = |h| \geq n$: $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ iff $||\mathfrak{h}|| \geq n$, by Proposition 1. Since $n \leq \mathcal{N}(\phi)$, we have $||\mathfrak{h}|| \geq n \Leftrightarrow n \leq \min(||\mathfrak{h}||, \mathcal{N}(\phi)) \Leftrightarrow \mathfrak{a}^{\mathfrak{i}}_n = \top^{\mathfrak{i}} \Leftrightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\phi)$.
– $\phi = |U| \geq n$: $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ iff $||\mathfrak{U}|| \geq n$, by Proposition 1. Since $n \leq \mathcal{N}(\phi)$, we have $||\mathfrak{U}|| \geq n \Leftrightarrow n \leq \min(||\mathfrak{U}||, \mathcal{N}(\phi)) \Leftrightarrow \mathfrak{b}^{\mathfrak{i}}_n = \top^{\mathfrak{i}} \Leftrightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\phi)$.
– $\phi = |h| \geq |U| - n$: $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ iff $||\mathfrak{h}|| \geq ||\mathfrak{U}|| - n$, by Proposition 1. Equivalently, $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg\phi$ iff $n + 1 \leq ||\mathfrak{U}|| - ||\mathfrak{h}||$. Since $n + 1 \leq \mathcal{N}(\phi) + 1$, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg\phi \Leftrightarrow n + 1 \leq \min(||\mathfrak{U}|| - ||\mathfrak{h}||, \mathcal{N}(\phi) + 1) \Leftrightarrow \mathfrak{c}^{\mathfrak{i}}_{n+1} = \top^{\mathfrak{i}}$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi \Leftrightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \neg c_{n+1} \Leftrightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\phi)$.
– $\phi = x \hookrightarrow (y_1, \ldots, y_k)$: $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ iff $\mathfrak{h}(\mathfrak{s}(x)) = (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))$ iff $\mathfrak{p}^{\mathfrak{i}}(\mathfrak{s}(x), \mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k)) = \top^{\mathfrak{i}}$ iff $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \mathfrak{p}(x, y_1, \ldots, y_k)$.
– $\phi = \mathsf{alloc}(x)$: $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ iff $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h})$ iff $\mathfrak{h}(\mathfrak{s}(x)) = (\ell_1, \ldots, \ell_k)$, for some $\ell_1, \ldots, \ell_k \in \mathfrak{U}$ iff $\mathfrak{p}^{\mathfrak{i}}(\mathfrak{s}(x), \ell_1, \ldots, \ell_k) = \top^{\mathfrak{i}}$, for some $\ell_1, \ldots, \ell_k \in \mathfrak{U}$ iff $(\mathfrak{U}, \mathfrak{s}[y_1 \leftarrow \ell_1] \ldots [y_k \leftarrow \ell_k], \mathfrak{i}) \models \mathfrak{p}(x, y_1, \ldots, y_k)$, for some $\ell_1, \ldots, \ell_k \in \mathfrak{U}$ iff $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \exists y_1 \ldots \exists y_k \,.\, \mathfrak{p}(x, y_1, \ldots, y_k)$.
– the cases $\phi = \phi_1 \wedge \phi_2$, $\phi = \neg\phi_1$ and $\phi = \exists x \,.\, \phi_1$ are by the inductive hypothesis, since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi_i \Leftrightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\phi_i)$, for all $i = 1, 2$.

(2) Let $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$ be a model of $\tau(\phi) \wedge \mathcal{A}(\phi)$, such that $||\mathfrak{p}^{\mathfrak{i}}|| \in \mathbb{N}$. We define a heap $\mathfrak{h}$ as follows: for each $(k + 1)$-tuple of locations $\ell_0, \ldots, \ell_k \in \mathfrak{U}$ such that $\mathfrak{p}^{\mathfrak{i}}(\ell_0, \ldots, \ell_k) = \top^{\mathfrak{i}}$, we set $\mathfrak{h}(\ell_0) = (\ell_1, \ldots, \ell_k)$. Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models P$ and $||\mathfrak{p}^{\mathfrak{i}}|| \in \mathbb{N}$, we obtain that $\mathfrak{h}$ is a finite partial function. We prove that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\phi) \Rightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ by induction on the structure of the negation normal form of ϕ:

– $\phi = |h| \geq n$: $\tau(\phi) = \mathfrak{a}_n$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \mathfrak{a}_n \Rightarrow \mathfrak{a}^{\mathfrak{i}}_n = \top^{\mathfrak{i}}$. Since $n \leq \mathcal{N}(\phi)$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \bigwedge_{i=0}^{\mathcal{N}(\phi)} A_j$, we have $\mathfrak{a}^{\mathfrak{i}}_j = \top^{\mathfrak{i}}$ and $\mathfrak{u}^{\mathfrak{i}}_j \in \mathrm{dom}(\mathfrak{h})$, for all $j \in [1, n]$. Because $\mathfrak{u}^{\mathfrak{i}}_j$ are pairwise disjoint, for all $j \in [1, n]$, we obtain that $||\mathfrak{h}|| \geq n$, and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ follows, by Proposition 1.
– $\phi = |h| < n$: $\tau(\phi) = \neg\mathfrak{a}_n$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \neg\mathfrak{a}_n \Rightarrow \mathfrak{a}^{\mathfrak{i}}_n = \bot^{\mathfrak{i}}$. Since $n \leq \mathcal{N}(\phi)$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \bigwedge_{i=0}^{\mathcal{N}(\phi)} A_j$, we have that each location $\ell \in \mathrm{dom}(\mathfrak{h})$ must be one of $\mathfrak{u}^{\mathfrak{i}}_1, \ldots, \mathfrak{u}^{\mathfrak{i}}_{n-1}$, thus $||\mathrm{dom}(\mathfrak{h})|| \leq n - 1$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models |h| < n$ follows, by Proposition 1.
– $\phi = |U| \geq n$: $\tau(\phi) = \mathfrak{b}_n$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \mathfrak{b}_n \Rightarrow \mathfrak{b}^{\mathfrak{i}}_n = \top^{\mathfrak{i}}$. Since $n \leq \mathcal{N}(\phi)$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \bigwedge_{i=0}^{\mathcal{N}(\phi)} B_j$, we have $\mathfrak{b}^{\mathfrak{i}}_j = \top^{\mathfrak{i}}$, for all $j \in [1, n]$. Because $\mathfrak{v}^{\mathfrak{i}}_j$ are pairwise disjoint, for all $j \in [1, n]$, we obtain that $||\mathfrak{U}|| \geq n$, and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ follows, by Proposition 1.
– $\phi = |U| < n$: $\tau(\phi) = \neg\mathfrak{b}_n$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \neg\mathfrak{b}_n \Rightarrow \mathfrak{b}^{\mathfrak{i}}_n = \bot^{\mathfrak{i}}$. Since $n \leq \mathcal{N}(\phi)$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \bigwedge_{i=0}^{\mathcal{N}(\phi)} B_j$, we have that each location $\ell \in \mathfrak{U}$ must be one of $\mathfrak{v}^{\mathfrak{i}}_1, \ldots, \mathfrak{v}^{\mathfrak{i}}_{n-1}$, thus $||\mathfrak{U}|| \leq n - 1$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ follows, by Proposition 1.

– $\phi = |h| \geq |U| - n$: this case is impossible because $|h| \geq |U| - n$ must occur at negative polarity in ϕ.
– $\phi = |h| < |U| - n$: $\tau(\phi) = \mathfrak{c}_{n+1}$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \mathfrak{c}_{n+1} \Rightarrow \mathfrak{c}_{n+1} = \top^{\mathfrak{i}}$. Since $n + 1 \leq \mathcal{N}(\phi) + 1$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \bigwedge_{i=0}^{\mathcal{N}(\phi)+1} C_j$, we obtain that $\mathfrak{w}_j^{\mathfrak{i}} \in \mathfrak{U} \setminus \mathrm{dom}(\mathfrak{h})$, for all $j \in [1, n + 1]$. Since $\mathfrak{w}_j^{\mathfrak{i}}$ are pairwise disjoint, we obtain $||U|| - ||\mathfrak{h}|| \geq n + 1$ thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \phi$ follows, by Proposition 1.
– $\phi \in \{x \hookrightarrow (y_1, \ldots, y_k), \neg x \hookrightarrow (y_1, \ldots, y_k), \mathsf{alloc}(x), \neg\mathsf{alloc}(x)\}$: $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models x \hookrightarrow (y_1, \ldots, y_k) \Leftrightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \mathfrak{p}(x, y_1, \ldots, y_k)$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{alloc}(x) \Leftrightarrow (\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \exists y_1 \ldots y_k \,.\, \mathfrak{p}(x, y_1, \ldots, y_k)$ are proved in the same way as for point (1).
– the cases $\phi = \phi_1 \wedge \phi_2$, $\phi = \phi_1 \vee \phi_2$, $\exists x \,.\, \phi_1$ are by inductive hypothesis. □

Proposition 4. *Let* $\forall x.\phi[\exists y.\psi]$ *be a* FO *formula, such that* $\exists y.\psi$ *occurs at a positive polarity in* ϕ*. If* $x \notin \mathsf{var}(\psi)$ *and* $y \notin \mathsf{var}(\phi)$ *then* $\forall x.\phi[\exists y.\psi] \equiv \exists y \forall x.\phi[\psi/\exists y.\psi]$.

Proof: $\boxed{\forall x.\phi[\exists y.\psi] \models \exists y \forall x.\phi[\psi/\exists y.\psi]}$ Let $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$ be a model of $\forall x.\phi[\exists y.\psi]$ and let $t \in \{\bot, \top\}$ be the boolean constant such that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \exists y.\psi \leftrightarrow t$. Since $x \notin \mathsf{var}(\psi)$, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \forall x.\phi[t/\exists y.\psi]$ and moreover $(\mathfrak{U}, \mathfrak{s}[y \leftarrow \ell], \mathfrak{i}) \models \psi \leftrightarrow t$, for some location $\ell \in \mathfrak{U}$. Since $y \notin \mathsf{var}(\forall x.\phi[t/\exists y.\psi])$, we also have $(\mathfrak{U}, \mathfrak{s}[y \leftarrow \ell], \mathfrak{i}) \models \forall x.\phi[\psi/\exists y.\psi]$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \exists y \forall x.\phi[\psi/\exists y.\psi]$.
$\boxed{\exists y \forall x.\phi[\psi/\exists y.\psi] \models \forall x.\phi[\exists y.\psi]}$ Let $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$ be a model of $\exists y \forall x.\phi[\psi/\exists y.\psi]$. Then $(\mathfrak{U}, \mathfrak{s}[y \leftarrow \ell], \mathfrak{i}) \models \forall x.\phi[\psi/\exists y.\psi]$, for some location $\ell \in \mathfrak{U}$. Let $t \in \{\top, \bot\}$ be the boolean constant such that $(\mathfrak{U}, \mathfrak{s}[y \leftarrow \ell], \mathfrak{i}) \models t \leftrightarrow \psi$. We distinguish the following cases:
– $t = \bot$: since t occurs positively in $\phi[t/\exists y.\psi]$ by hypothesis, we have $(\mathfrak{U}, \mathfrak{s}[y \leftarrow \ell], \mathfrak{i}) \models \forall x.\phi[\exists y.\psi]$;
– $t = \top$: $(\mathfrak{U}, \mathfrak{s}[y \leftarrow \ell], \mathfrak{i}) \models \exists y.\psi \leftrightarrow \top$ hence $(\mathfrak{U}, \mathfrak{s}[y \leftarrow \ell], \mathfrak{i}) \models \forall x.\phi[\exists y.\psi]$.

In both cases $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \forall x.\phi[\exists y.\psi]$ follows because $y \notin \mathsf{var}(\phi)$. □

We end this section by delimiting a fragment of SL^k whose translation into FO falls into BSR(FO).

Lemma 2. *Given an* SL^k *formula* $\varphi = \forall y_1 \ldots \forall y_m \,.\, \phi$*, where* ϕ *is a boolean combination of test formulae containing no positive occurrence of* $\mathsf{alloc}(y_i)$*, for any* $i \in [1, m]$*,* $\tau(\varphi)$ *is equivalent to a* BSR(FO) *formula with the same constants and free variables as* $\tau(\varphi)$*.*

Proof: By definition of $\tau(.)$, we have $\tau(\varphi) = \forall y_1 \ldots \forall y_m \,.\, \tau(\phi)$ and the only existential quantifiers in $\tau(\varphi)$ are those in the formulae $\exists z_1 \ldots \exists z_k \,.\, \mathfrak{p}(x, z_1, \ldots, z_k)$ introduced by translating formulae of the form $\mathsf{alloc}(x)$ occurring positively in ϕ. Since ϕ contains no positive occurrence of $\mathsf{alloc}(y_i)$ by hypothesis, $x \notin \{y_1, \ldots, y_m\}$. Consequently, for all $i \in [1, m]$, y_i does not occur as an argument of $\mathfrak{p}$ and by Proposition 4, the quantifiers $\exists z_1 \ldots \exists z_k$ may be shifted to the root of the formula $\tau(\varphi)$ without affecting equivalence. By repeating this operation for each formula $\mathsf{alloc}(x)$ in ϕ, we eventually get a formula in $\mathsf{BSR}(\mathsf{FO})$. □

4 From Quantifier-free SL^k to Test Formulae

This section gives the expressive completeness result of the paper, namely that any quantifier-free SL^k formula is equivalent, on both finite and infinite models, to a quantifier-free boolean combination of test formulae. Starting from a quantifier-free SL^k formula φ, we define, inductively on the structure of φ, a set $\mu(\varphi)$ of conjunctions of test formulae and their negations, called *minterms*, such that $\varphi \equiv \bigvee_{M \in \mu(\varphi)} M$. Although the number of minterms in $\mu(\varphi)$ is, in general, exponential in the size of φ, checking the membership of a given minterm M in $\mu(\varphi)$ can be done in PSPACE. Together with the translation of minterms into FO (§3.1), this fact is used to prove PSPACE membership of the two decidable fragments of $\mathsf{BSR}(\mathsf{SL}^k)$, defined next (§5.2).

In the rest of this section we view a conjunction T of literals as a set[6], thus we use the same symbol to denote both a set and the formula obtained by conjoining the elements of the set. We define $\mathsf{var}(T) \stackrel{\text{def}}{=} \bigcup_{\ell \in T} \mathsf{var}(\ell)$. The equivalence relation $x \approx_T y$ is defined as $T \models x \approx y$ and we write $x \not\approx_T y$ for $T \models \neg x \approx y$. Observe that $x \not\approx_T y$ is not the complement of $x \approx_T y$. For a set X of variables, $|X|_T$ is the number of equivalence classes of $\approx_T$ in X.

4.1 Minterms

A *minterm* M is a set (conjunction) of literals containing:

- exactly one literal $|h| \geq \min_M$ and one literal $|h| < \max_M$, where $\min_M \in \mathbb{N} \cup \{|U| - n \mid n \in \mathbb{N}\}$ and $\max_M \in \mathbb{N}_\infty \cup \{|U| - n \mid n \in \mathbb{N}\}$, and
- at most[7] one literal of the form $|U| \geq n$, respectively $|U| < n$.

For an SL-structure $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$, let $\min_M^{\mathcal{I}}, \max_M^{\mathcal{I}} \in \mathbb{N}_\infty$ be the values obtained by replacing $|U|$ with $||\mathfrak{U}||$ in $\min_M$ and $\max_M$, respectively.

Definition 5. *Given a minterm M, we define the sets:*

$$M^e \stackrel{\text{def}}{=} M \cap \{x \approx y, \neg x \approx y \mid x, y \in \mathsf{Var}\}$$
$$M^a \stackrel{\text{def}}{=} M \cap \{\mathsf{alloc}(x), \neg \mathsf{alloc}(x) \mid x \in \mathsf{Var}\}$$
$$M^u \stackrel{\text{def}}{=} M \cap \{|U| \geq n, |U| < n \mid n \in \mathbb{N}\}$$
$$M^p \stackrel{\text{def}}{=} M \cap \{x \hookrightarrow \mathbf{y}, \neg x \hookrightarrow \mathbf{y} \mid x \in \mathsf{Var}, \mathbf{y} \in \mathsf{Var}^k\}$$

[6] The empty set is thus considered to be true.

[7] This condition is not restrictive: if M contains two literals $|U| \geq n_1$ and $|U| \geq n_2$ with $n_1 < n_2$ then $|U| \geq n_1$ is redundant and can be removed.

Thus, $M = M^e \cup M^u \cup M^a \cup M^p \cup \{|h| \geq \min_M, |h| < \max_M\}$, for each minterm M.

Proposition 5. *Given a minterm M, for all structures $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ and $\mathcal{I}' = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h}')$ we have $\mathcal{I} \models M^e \wedge M^u \Leftrightarrow \mathcal{I}' \models M^e \wedge M^u$.*

Proof: The test formulae in $M^e \cup M^u$ do not depend on the heap. □

Given a set of variables $X \subseteq \mathsf{Var}$, a minterm M is (1) *E-complete* for X iff for all $x, y \in X$ exactly one of $x \approx y \in M$, $\neg x \approx y \in M$ holds, and (2) *A-complete* for X iff for each $x \in X$ exactly one of $\mathsf{alloc}(x) \in M$, $\neg\mathsf{alloc}(x) \in M$ holds.

Proposition 6. *If M is E-complete for $\mathsf{var}(M)$, $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models M$ and $X \subseteq \mathsf{var}(M)$, then $|X|_M = ||\mathfrak{s}(\mathsf{var}(M))||$.*

Proof: This is an immediate consequence of the fact that if $x, x' \in \mathsf{var}(M)$, then $\mathfrak{s}(x) = \mathfrak{s}(x')$ if and only if $M \models x \approx x'$. □

For a literal ℓ, we denote by $\overline{\ell}$ its complement, i.e. $\overline{\theta} \stackrel{\text{def}}{=} \neg\theta$ and $\overline{\neg\theta} \stackrel{\text{def}}{=} \theta$, where θ is a test formula. Let $\overline{M}$ be the minterm obtained from M by replacing each literal with its complement. The *complement closure* of M is $\mathsf{cc}(M) \stackrel{\text{def}}{=} M \cup \overline{M}$.

Two tuples $\mathbf{y}, \mathbf{y}' \in \mathsf{Var}^k$ are *M-distinct* if $y_i \not\approx_M y'_i$, for some $i \in [1, k]$. Given a minterm M that is E-complete for $\mathsf{var}(M)$, its *points-to closure* is $\mathsf{pc}(M) \stackrel{\text{def}}{=} \bot$ if there exist literals $x \hookrightarrow \mathbf{y}, x' \hookrightarrow \mathbf{y}' \in M$ such that $x \approx_M x'$ and $\mathbf{y}, \mathbf{y}'$ are M-distinct, and $\mathsf{pc}(M) = M$, otherwise. Intuitively, $\mathsf{pc}(M)$ is $\bot$ iff M contradicts the fact that the heap is a partial function. Note that we do not assert the equality $\mathbf{y} \approx \mathbf{y}'$, instead we only check that it is not falsified. This is sufficient for our purpose because in the following we always assume that the considered minterms are E-complete.

The *domain closure* of M is $\mathsf{dc}(M) \stackrel{\text{def}}{=} \bot$ if either $\min_M = n_1$ and $\max_M = n_2$ for some $n_1, n_2 \in \mathbb{Z}$ such that $n_1 \geq n_2$, or $\min_M = |U| - n_1$ and $\max_M = |U| - n_2$, where $n_2 \geq n_1$; and otherwise:

$$\begin{aligned} \mathsf{dc}(M) \stackrel{\text{def}}{=} M &\cup \left\{|U| \geq \left\lceil \sqrt[k]{\max_{x \in \mathsf{av}(M)}(\delta_x(M) + 1)} \right\rceil\right\} \\ &\cup \{|U| \geq n_1 + n_2 + 1 \mid \min_M = n_1, \max_M = |U| - n_2, n_1, n_2 \in \mathbb{N}\} \\ &\cup \{|U| < n_1 + n_2 \mid \min_M = |U| - n_1, \max_M = n_2, n_1, n_2 \in \mathbb{N}\} \end{aligned}$$

where $\delta_x(M)$ is the number of pairwise M-distinct tuples $\mathbf{y}$ for which there exists $\neg x' \hookrightarrow \mathbf{y} \in M$ such that $x \approx_M x'$. Intuitively, $\mathsf{dc}(M)$ asserts that $\min_M < \max_M$ and that the domain contains enough elements to allocate all cells. Moreover, for every allocated variable x, there must exist at least $\delta_x(M) + 1$ distinct k-vectors of elements of the domain: the $\delta_x(M)$ that x cannot point to, plus the image of x. For instance, if $M = \{\neg x \hookrightarrow y_i, \mathsf{alloc}(x), y_i \not\approx y_j \mid i, j \in [1, n], i \neq j\}$, then it is clear that M is unsatisfiable if there are less than n locations, since x cannot be allocated in this case.

Proposition 7. *For any minterm M, we have $M \equiv \mathsf{pc}(M) \equiv \mathsf{dc}(M)$.*

Proof: It is manifest that $\mathsf{pc}(M) \models M$ and $\mathsf{dc}(M) \models M$. Let $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ be a model of M. Then for each two variables $x, x' \in \mathsf{var}(M)$ such that $x \hookrightarrow (y_1, \ldots, y_k), x' \hookrightarrow (z_1, \ldots, z_k) \in M$ and $x \approx_M x'$, we have $\mathfrak{h}(\mathfrak{s}(x)) = (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))$, $\mathfrak{h}(\mathfrak{s}(x')) = (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))$ and $\mathfrak{h}(\mathfrak{s}(x)) = \mathfrak{h}(\mathfrak{s}(x'))$, thus $\mathfrak{s}(y_i) = \mathfrak{s}(z_i)$, for all $i \in [1, k]$, thus $\mathcal{I} \models \mathsf{pc}(M)$. For a variable $x \in \mathsf{av}(M)$, let $x_1 \not\hookrightarrow \mathbf{y}_1, \ldots, x_n \not\hookrightarrow \mathbf{y}_n \in M$ be all literals such that $x_1 \approx_M \ldots \approx_M x_n \approx_M x$ and $\mathbf{y}_i \not\approx_M \mathbf{y}_j$ for all $i \neq j$. Then $\mathfrak{h}(\mathfrak{s}(x)) \in \mathfrak{U}^k \setminus \{\mathfrak{s}(\mathbf{y}_1), \ldots, \mathfrak{s}(\mathbf{y}_n)\}$, thus $||\mathfrak{U}||^k \geq n+1 = \delta_x(M)+1$. Since this holds for each $x \in \mathsf{av}(M)$, we have $\mathcal{I} \models |U| \geq \left\lceil \sqrt[k]{\max_{x \in \mathsf{av}(M)}(\delta_x(M) + 1)} \right\rceil$. Further, if $\mathcal{I} \models M$ and $|h| \geq n_1, |h| < |U| - n_2 \in M$ then $||\mathfrak{U}|| - n_2 > ||\mathfrak{h}|| \geq n_1$, thus $||U|| \geq n_1 + n_2 + 1$ and $\mathcal{I} \models |U| \geq n_1 + n_2 + 1$. Analogously, we obtain $\mathcal{I} \models |U| < n_1 + n_2$ in the case $|h| < n_1, |h| \geq |U| - n_2 \in M$. □

Proposition 8. *Given a minterm M, $\min^{\mathcal{I}}_M < \max^{\mathcal{I}}_M$ for any model $\mathcal{I}$ of $\mathsf{dc}(M)^u$.*

Proof: Let $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ and $n_1, n_2 \in \mathbb{N}_\infty$. We distinguish the following cases:

- if $\min_M = n_1$ and $\max_M = n_2$ then $n_1 \geq n_2$ must be the case, or else $\mathsf{dc}(M) \equiv \bot$, in contradiction with $\mathcal{I} \models \mathsf{dc}(M)^u$.
- if $\min_M = n_1$ and $\max_M = |U| - n_2$ then $|U| \geq n_1 + n_2 + 1 \in \mathsf{dc}(M)$ and since $\mathcal{I} \models \mathsf{dc}(M)^u$, we obtain $n_1 < ||\mathfrak{U}|| - n_2$.
- if $\min_M = |U| - n_1$ and $\max_M = n_2$ then $|U| < n_1 + n_2 \in \mathsf{dc}(M)$ and since $\mathcal{I} \models \mathsf{dc}(M^u)$, we obtain $||\mathfrak{U}|| - n_1 < n_2$.
- if $\min_M = |U| - n_1$ and $\max_M = |U| - n_2$ then $n_2 < n_1$ must be the case, or else $\mathsf{dc}(M) \equiv \bot$, in contradiction with $\mathcal{I} \models \mathsf{dc}(M)^u$. □

Definition 6. *A minterm M is* footprint-consistent *if for all $x, x' \in \mathsf{Var}$ and $\mathbf{y}, \mathbf{y}' \in \mathsf{Var}^k$, such that $x \approx_M x'$ and $y_i \approx_M y'_i$ for all $i \in [1, k]$, we have (1) if $\mathsf{alloc}(x) \in M$ then $\neg\mathsf{alloc}(x') \notin M$, and (2) if $x \hookrightarrow \mathbf{y} \in M$ then $\neg\mathsf{alloc}(x'), \neg x' \hookrightarrow \mathbf{y}' \notin M$.*

Note that footprint-consistency is a necessary, yet not sufficient, condition for satisfiability of minterms. For example, the minterm $M = \{x \hookrightarrow y, x' \hookrightarrow y', \neg y \approx y', |h| < 2\}$ is at the same time footprint-consistent and unsatisfiable.

Proposition 9. *If M is a footprint-consistent minterm, then $\mathsf{nv}(M) \cap \mathsf{av}(M) = \emptyset$. If, moreover, M is E-complete for $\mathsf{var}(M)$, then $\mathfrak{s}(X) \cap \mathfrak{s}(\mathsf{av}(M)) = \emptyset$ for each set X disjoint from $\mathsf{av}(M)$ and each model $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ of M.*

Proof: Suppose first that $x \in \mathsf{nv}(M) \cap \mathsf{av}(M)$. Then there exists literals $\neg\mathsf{alloc}(x')$ and $\mathsf{alloc}(x'')$ in M such that $x \approx_M x'$ and $x \approx_M x''$, which contradicts the footprint consistency of M. For the second point, suppose that $\ell \in \mathfrak{s}(X) \cap \mathfrak{s}(\mathsf{av}(M))$. Then there exists variables $x \in X$ and $x' \in \mathsf{av}(M)$ such that $\mathfrak{s}(x) = \mathfrak{s}(x') = \ell$. If

M is E-complete, either $x \approx x' \in M$ or $\neg x \approx x' \in M$. The first case contradicts $x \notin \mathsf{av}(M)$ and the second case contradicts $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models M$. $\square$

We are now ready to define a boolean combination of test formulae that is equivalent to $M_1 * M_2$, where M_1 and M_2 are minterms satisfying a number of additional conditions. Let $\mathsf{npto}(M_1, M_2) \stackrel{\text{def}}{=} (M_1 \cap M_2) \cap \{\neg x \hookrightarrow \mathbf{y} \mid x \notin \mathsf{av}(M_1 \cup M_2), \mathbf{y} \in \mathsf{Var}^k\}$ be the set of negative points-to literals common to M_1 and M_2, involving left-hand side variables not allocated in either M_1 or M_2.

Lemma 3. *Let M_1 and M_2 be two minterms that are footprint-consistent and E-complete for $\mathsf{var}(M_1 \cup M_2)$, with $\mathsf{cc}(M_1^p) = \mathsf{cc}(M_2^p)$. Then $M_1 * M_2 \equiv \mathsf{elim}_*(M_1, M_2)$, where $\mathsf{elim}_*(M_1, M_2)$ is:*

$$M_1^e \wedge M_2^e \wedge \mathsf{dc}(M_1)^u \wedge \mathsf{dc}(M_2)^u \wedge \tag{1}$$

$$\bigwedge_{x \in \mathsf{av}(M_1),\ y \in \mathsf{av}(M_2)} \neg x \approx y \wedge \mathsf{fp}_a(M_1) \wedge \mathsf{fp}_a(M_2) \wedge \tag{2}$$

$$\mathsf{nalloc}(\mathsf{nv}(M_1) \cap \mathsf{nv}(M_2)) \wedge \mathsf{npto}(M_1, M_2) \wedge \tag{3}$$

$$|h| \geq \min_{M_1} + \min_{M_2} \ \wedge\ |h| < \max_{M_1} + \max_{M_2} - 1 \tag{4}$$

$$\wedge\ \eta_{12} \wedge \eta_{21} \tag{5}$$

where $\eta_{ij} \stackrel{\text{def}}{=}$

$$\bigwedge_{Y \subseteq \mathsf{nv}(M_j) \setminus \mathsf{av}(M_i)} \mathsf{alloc}(Y) \rightarrow \begin{pmatrix} |h| \geq \#_a(M_i) + |Y|_{M_i} + \min_{M_j} \\ \wedge\ \#_a(M_i) + |Y|_{M_i} < \max_{M_i} \end{pmatrix}$$

Intuitively, if M_1 and M_2 hold separately, then all heap-independent literals from $M_1 \cup M_2$ must be satisfied (1), the variables allocated in M_1 and M_2 must be pairwise distinct and their footprints, relative to the allocated variables, jointly asserted (2). Moreover, unallocated variables on both sides must not be allocated and common negative points-to literals must be asserted (3). Since the heap satisfying $\mathsf{elim}_*(M_1, M_2)$ is the disjoint union of the heaps for M_1 and M_2, its bounds are the sum of the bounds on both sides (4) and, moreover, the variables that M_2 never allocates [$\mathsf{nv}(M_2)$] may occur allocated in the heap of M_1 and viceversa, thus the constraints η_{12} and η_{21}, respectively (5).

Proof: Suppose first that $M_1^e \neq M_2^e$. Since M_1 and M_2 are E-complete for $\mathsf{var}(M_1 \cup M_2)$, there must exist a literal $x \approx y \in M_1^e$ such that $\neg x \approx y \in M_2^e$, or viceversa. In both cases however $M_1 * M_2 \equiv \mathsf{elim}_*(M_1, M_2) \equiv \bot$. Thus we consider from now on that $M_1^e = M_2^e$.

$\boxed{M_1 * M_2 \models \mathsf{elim}_*(M_1, M_2)}$ Let $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ be a model of $M_1 * M_2$. Then there exists disjoint heaps $\mathfrak{h}_1$ and $\mathfrak{h}_2$ such that $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_i) \models M_i$, for all $i = 1, 2$. Below we show that $\mathcal{I}$ is a model of the formulae (1), (2), (3), (4) and (5).

(1) Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_i) \models M_i^e \wedge M_i^u$, by Proposition 5, we also have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models M_i^e \wedge M_i^u$, for $i = 1, 2$. By Proposition 7, we obtain further that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{dc}(M_i)^u$, for $i = 1, 2$.

(2) Since $\mathrm{dom}(\mathfrak{h}_1) \cap \mathrm{dom}(\mathfrak{h}_2) = \emptyset$, for every $x \in \mathsf{av}(M_1)$ and $y \in \mathsf{av}(M_2)$, we must have $\mathfrak{s}(x) \neq \mathfrak{s}(y)$, hence $\mathcal{I} \models \neg x \approx y$. Further, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_i) \models M_i$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_i) \models \mathsf{fp}_a(M_i)$ and, by Proposition 3, $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{fp}_a(M_i)$, for all $i = 1, 2$.

(3) Let $x \in \mathsf{nv}(M_1) \cap \mathsf{nv}(M_2)$ be a variable. Then there exists variables x_1 and x_2 such that $\neg\mathsf{alloc}(x_1) \in M_1$, $x \approx_{M_1} x_1$, $\neg\mathsf{alloc}(x_2) \in M_2$ and $x \approx_{M_2} x_2$. Hence $\mathfrak{s}(x) = \mathfrak{s}(x_1) \notin \mathrm{dom}(\mathfrak{h}_1)$ and $\mathfrak{s}(x) = \mathfrak{s}(x_2) \notin \mathrm{dom}(\mathfrak{h}_2)$, thus $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h})$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg\mathsf{alloc}(x)$. Since x was chosen arbitrarily, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{nalloc}(\mathsf{nv}(M_1) \cap \mathsf{nv}(M_2))$. Secondly, let $\neg x \hookrightarrow \mathbf{y} \in M_1 \cap M_2$, for some $x \notin \mathsf{av}(M_1 \cup M_2)$. Since $\mathrm{dom}(\mathfrak{h}_1) \cap \mathrm{dom}(\mathfrak{h}_2) = \emptyset$, only the following are possible:

1. $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h}_1)$. Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models M_1$, we must have $\mathfrak{h}_1(x) \neq \mathfrak{s}(\mathbf{y})$. Then $\mathfrak{h}(x) \neq \mathfrak{s}(\mathbf{y})$ thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg x \hookrightarrow \mathbf{y}$.
2. $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h}_2)$ and $\mathfrak{h}_2(x) \neq \mathfrak{s}(\mathbf{y})$ is symmetrical.
3. $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h}_1) \cup \mathrm{dom}(\mathfrak{h}_2)$, then $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h})$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg x \hookrightarrow \mathbf{y}$.

Since $\neg x \hookrightarrow \mathbf{y} \in \mathsf{npto}(M_1, M_2)$ was chosen arbitrarily, $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{npto}(M_1, M_2)$.

(4) Since $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$, we have $||\mathfrak{h}|| = ||\mathfrak{h}_1|| + ||\mathfrak{h}_2||$, thus the first two constraints are obtained by summing up the constraints $\min^{\mathcal{I}}_{M_i} \leq ||\mathfrak{h}_i|| < \max^{\mathcal{I}}_{M_i}$, for $i = 1, 2$.

(5) We prove $\mathcal{I} \models \eta_{12}$, the proof for $\mathcal{I} \models \eta_{21}$ being symmetrical. Consider a set $Y \subseteq \mathsf{nv}(M_2) \setminus \mathsf{av}(M_1)$ and suppose that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{alloc}(Y)$. For each $y \in Y$ we must have $\mathfrak{s}(y) \in \mathrm{dom}(\mathfrak{h}_1)$, because $\mathfrak{s}(y) \notin \mathrm{dom}(\mathfrak{h}_2)$ and $\mathfrak{s}(y) \in \mathrm{dom}(\mathfrak{h})$. Moreover, $\mathfrak{s}(Y) \cap \mathfrak{s}(\mathsf{av}(M_1)) = \emptyset$ because $Y \cap \mathsf{av}(M_1) = \emptyset$ and M_1 is E-complete for $\mathsf{var}(M_1 \cup M_2)$, by Proposition 9. Thus $\#_a(M_1) + |Y|_{M_1} \leq ||\mathfrak{h}_1|| < \max^{\mathcal{I}}_{M_1}$ and $||\mathfrak{h}|| = ||\mathfrak{h}_1|| + ||\mathfrak{h}_2|| \geq \#_a(M_1) + |Y|_{M_1} + \min^{\mathcal{I}}_{M_2}$, as required.

$\boxed{\mathsf{elim}_*(M_1, M_2) \models M_1 * M_2}$ Let $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ be a model of $\mathsf{elim}_*(M_1, M_2)$. We shall find $\mathfrak{h}_1$ and $\mathfrak{h}_2$ such that $\mathfrak{h} = \mathfrak{h}_1 \uplus \mathfrak{h}_2$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_i) \models M_i$, for all $i = 1, 2$. Since $\mathcal{I} \models \min_{M_1} + \min_{M_2} \leq |h| \wedge |h| < \max_{M_1} + \max_{M_2} - 1$ by (4), we have, by Proposition 1:

$$\min^{\mathcal{I}}_{M_1} + \min^{\mathcal{I}}_{M_2} \leq ||\mathfrak{h}|| < \max^{\mathcal{I}}_{M_1} + \max^{\mathcal{I}}_{M_2} - 1 \tag{6}$$

Let us now define the following sets, for $i = 1, 2$:

$$L_i = \{\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h}) \mid x \in \mathsf{nv}(M_{3-i}) \setminus \mathsf{av}(M_i)\}$$
$$Y_i = \{x \in \mathsf{Var} \mid \mathfrak{s}(x) \in L_i\}$$
$$A_i = \{\mathfrak{s}(x) \mid x \in \mathsf{av}(M_i)\}$$

First, we prove that $L_1 \cap L_2 = \emptyset$. By contradiction, suppose that there exists $\ell \in L_1 \cap L_2$. Then $\ell = \mathfrak{s}(y_1) = \mathfrak{s}(y_2)$ for some $y_1 \in \mathsf{nv}(M_1)$ and $y_2 \in \mathsf{nv}(M_2)$. Because M_1 is E-complete for $\mathsf{var}(M_1 \cup M_2)$, exactly one of $y_1 \approx y_2$, $\neg y_1 \approx y_2$

belongs to M_1. But $\neg y_1 \approx y_2 \in M_1$ contradicts with $\mathfrak{s}(y_1) = \mathfrak{s}(y_2)$ and $y_1 \approx y_2 \in M_1$ leads to $y_2 \in \mathsf{nv}(M_1)$. Symmetrically, $y_1 \in \mathsf{nv}(M_2)$, thus $y_1, y_2 \in \mathsf{nalloc}(\mathsf{nv}(M_1) \cap \mathsf{nv}(M_2))$. Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{nalloc}(\mathsf{nv}(M_1) \cap \mathsf{nv}(M_2))$ by (3), we have $\ell \notin \mathrm{dom}(\mathfrak{h})$, which contradicts with the fact that $L_1 \cup L_2 \subseteq \mathrm{dom}(\mathfrak{h})$, according to the definition of L_1 and L_2.

Next, we show that $L_i \cap (A_1 \cup A_2) = \emptyset$, for $i = 1, 2$. First, $L_i \cap A_i = \emptyset$ because M_i are E-complete for $\mathsf{var}(M_1 \cup M_2)$, by Proposition 9. Second, $L_i \cap A_{3-i} = \emptyset$ because M_i are E-complete for $\mathsf{var}(M_1 \cup M_2)$ and $\mathsf{nv}(M_{3-i}) \cap \mathsf{av}(M_{3-i}) = \emptyset$, by Proposition 9.

Moreover $\mathcal{I} \models \mathsf{alloc}(Y_1) \wedge \mathsf{alloc}(Y_2)$ because $L_1 \cup L_2 \subseteq \mathrm{dom}(\mathfrak{h})$ by definition and, because $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \eta_{12} \wedge \eta_{21}$, the following hold, for $i = 1, 2$:

$$||\mathfrak{h}|| \geq ||A_i|| + ||L_i|| + \min^{\mathcal{I}}_{M_{3-i}} \quad (7) \qquad\qquad ||A_i|| + ||L_i|| < \max^{I}_{i} \quad (8)$$

We prove the following relation by distinguishing the cases below:

$$\max(\min^{\mathcal{I}}_{M_1}, ||A_1|| + ||L_1||) + \max(\min^{\mathcal{I}}_{M_2}, ||A_2|| + ||L_2||) \leq ||\mathfrak{h}|| \quad (9)$$

1. if $\min^{\mathcal{I}}_{M_1} \geq ||A_1|| + ||L_1||$ then we have $\min^{\mathcal{I}}_{M_1} + \max(\min^{\mathcal{I}}_{M_2}, ||A_2|| + ||L_2||) \leq ||\mathfrak{h}||$ by (4) and (7). The case $\min^{\mathcal{I}}_{M_2} \geq ||A_2|| + ||L_2||$ is symmetric, and
2. otherwise, if $\min^{\mathcal{I}}_{M_1} < ||A_1|| + ||L_1||$ and $\min^{\mathcal{I}}_{M_2} < ||A_2|| + ||L_2||$, because $\mathcal{I} \models \bigwedge_{x \in \mathsf{av}(M_1),\, y \in \mathsf{av}(M_2)} \neg x \approx y$, the sets of locations L_1, L_2, A_1 and A_2 are pairwise disjoint and, since $L_1 \cup L_2 \cup A_1 \cup A_2 \subseteq \mathrm{dom}(\mathfrak{h})$, it must be the case that $||\mathfrak{h}|| \geq ||A_1|| + ||L_1|| + ||A_2|| + ||L_2||$.

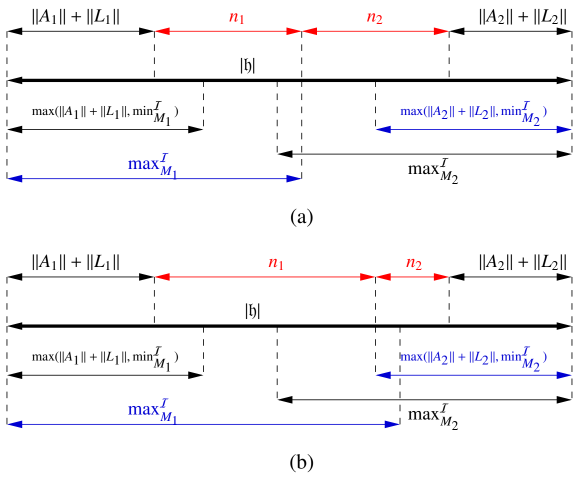

Fig. 1.

Furthermore, we have $||\mathfrak{h}|| < \max^{\mathcal{I}}_{M_1} + \max^{\mathcal{I}}_{M_2} - 1$ by (6) and one of the following cases occurs (see Fig. 1):

1. if $\max^{\mathcal{I}}_{M_1} - 1 \leq ||\mathfrak{h}|| - \max(||A_2|| + ||L_2||, \min^{\mathcal{I}}_{M_2})$ then let $n_1 = \max^{\mathcal{I}}_{M_1} - ||A_1|| - ||L_1|| - 1$ and $n_2 = ||\mathfrak{h}|| - \max^{\mathcal{I}}_{M_1} - ||A_2|| - ||L_2|| + 1$ (Fig. 1 (a)). We have that $n_1 \geq 0$ by (8) and $n_2 \geq 0$ by the hypothesis $\max^{\mathcal{I}}_{M_1} - 1 \leq ||\mathfrak{h}|| - \max(||A_2|| + ||L_2||, \min^{\mathcal{I}}_{M_2})$.
2. otherwise, let $n_1 = ||\mathfrak{h}|| - ||A_1|| - ||L_1|| - \max^{\mathcal{I}}(||A_2|| + ||L_2||, \min^{\mathcal{I}}_{M_2})$ and $n_2 = \max^{\mathcal{I}}(||A_2|| + ||L_2||, \min^{\mathcal{I}}_{M_2}) - ||A_2|| - ||L_2||$ (Fig. 1 (b)). We have $n_1 \geq 0$ by (9) and $n_2 \geq 0$ is immediate.

In both cases, the following holds, for $i = 1, 2$:

$$\min^{\mathcal{I}}_{M_i} \leq ||A_i|| + ||L_i|| + n_i < \max^{\mathcal{I}}_{M_i} \tag{10}$$

We have used the fact that $\min^{\mathcal{I}}_{M_i} < \max^{\mathcal{I}}_{M_i}$, for $i = 1, 2$, which is a consequence of the fact that $\mathcal{I} \models \mathsf{dc}(M_i)^u$, by (1) and Proposition 8.

Further, we have that $||\mathfrak{h}|| = \sum_{i=1,2} ||A_i|| + ||L_i|| + n_i$. Moreover, there are exactly $n_1 + n_2$ locations in $\mathrm{dom}(\mathfrak{h}) \setminus (A_1 \cup L_1 \cup A_2 \cup L_2)$, thus we can partition this set into N_1 and N_2 such that $||N_i|| = n_i$ and define $\mathfrak{h}_i$ to be the restriction of $\mathfrak{h}$ to $A_i \cup L_i \cup N_i$, for $i = 1, 2$. It remains to be shown that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_i) \models M_i$, for $i = 1, 2$. Below we do the proof for $i = 1$, the case $i = 2$ being symmetric.

Clearly, $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models M^u_1$, because $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \wedge\mathsf{dc}(M_1)^u$, by Proposition 5. Further, by (10) and Proposition 1, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models |h| \geq \min_{M_1} \wedge |h| < \max_{M_1}$. It remains to show that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models M^a_1 \wedge M^p_1$.

(M^a_1) Let $\mathsf{alloc}(x) \in M^a_1$ be a literal. Then $x \in \mathsf{av}(M_1)$, thus $\mathfrak{s}(x) \in A_1$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models \mathsf{alloc}(x)$ follows, by the definition of $\mathfrak{h}_1$. Dually, let $\neg\mathsf{alloc}(x) \in M^a_1$ be a literal. Then, we have $x \in \mathsf{nv}(M_1)$. We distinguish the cases:

- if $x \in \mathsf{av}(M_2)$ then $\mathfrak{s}(x) \in A_2$ and since $\mathrm{dom}(\mathfrak{h}_1) \cap A_2 = \emptyset$, we have $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h}_1)$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models \neg\mathsf{alloc}(x)$.
- otherwise, $x \in \mathsf{nv}(M_1) \setminus \mathsf{av}(M_2)$. Again, we distinguish the cases:
  - if $x \in Y_2$ then $\mathfrak{s}(x) \in L_2$ and because $\mathrm{dom}(\mathfrak{h}_1) \cap L_2 = \emptyset$, we obtain $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h}_1)$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models \neg\mathsf{alloc}(x)$.
  - otherwise, $x \notin Y_2$, thus $\mathfrak{s}(x) \notin L_2$. But since $x \in \mathsf{nv}(M_1) \setminus \mathsf{av}(M_2)$, by the definition of L_2, it must be the case that $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h})$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg\mathsf{alloc}(x)$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models \neg\mathsf{alloc}(x)$ follows.

(M^p_1) Let $x \hookrightarrow \mathbf{y} \in M^p_1$ be a literal. Then $x \in \mathsf{av}(M_1)$ and $\mathfrak{s}(x) \in A_1$. Moreover, we have $x \hookrightarrow \mathbf{y} \in \mathsf{fp}_a(M_1)$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models x \hookrightarrow \mathbf{y}$, by (2). Since $\mathfrak{h}$ and $\mathfrak{h}_1$ agree on A_1, we also have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models x \hookrightarrow \mathbf{y}$. Dually, let $\neg x \hookrightarrow \mathbf{y} \in M^p_1$. If $x \in \mathsf{av}(M_1)$ then $\neg x \hookrightarrow \mathbf{y} \in \mathsf{fp}_a(M_1)$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models \neg x \hookrightarrow \mathbf{y}$, since $\mathfrak{h}$ and $\mathfrak{h}_1$ agree on A_1. Otherwise, if $x \notin \mathsf{av}(M_1)$, we distinguish the cases:

– if $x \in \mathsf{av}(M_2)$ then $\mathfrak{s}(x) \in A_2$, and since $\mathrm{dom}(\mathfrak{h}_1) \cap A_2 = \emptyset$, we have $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h}_1)$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models \neg x \hookrightarrow \mathbf{y}$.
– otherwise, $x \notin \mathsf{av}(M_2)$, and since $\mathsf{cc}(M_1^p) = \mathsf{cc}(M_2^p)$, we have $\{x \hookrightarrow \mathbf{y}, \neg x \hookrightarrow \mathbf{y}\} \cap M_2 \neq \emptyset$. Since $x \notin \mathsf{av}(M_2)$, the only possibility is $\neg x \hookrightarrow \mathbf{y} \in M_2$, thus $\neg x \hookrightarrow \mathbf{y} \in \mathsf{npto}(M_1, M_2)$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg x \hookrightarrow \mathbf{y}$, by (3). Since $\mathfrak{h}$ is an extension of $\mathfrak{h}_1$, we obtain that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}_1) \models \neg x \hookrightarrow \mathbf{y}$ as well. □

Remark 3. Note that $\mathsf{elim}_*(M_1, M_2)$ introduces literals of the form $\neg\mathsf{alloc}(x)$ that do not occur in $M_1 \cup M_2$. For example, if $M_1 = \{\neg\mathsf{alloc}(x), x \approx y, |h| \geq 0, |h| < \infty\}$ and $M_2 = \{|h| \geq 0, |h| < \infty\}$, then $y \in \mathsf{nv}(M_1)$ and $\mathsf{alloc}(y)$ occurs at negative polarity in $\mathsf{elim}_*(M_1, M_2)$. This is problematic because upcoming results depend on the fact that the polarity of $\mathsf{alloc}(x)$ formulae is preserved (Lemma 6). Moreover, if $\neg\mathsf{alloc}(x) \in \mathsf{elim}_*(M_1, M_2)$, then there exists a literal $\neg\mathsf{alloc}(x') \in M_1 \cup M_2$, such that $\mathsf{elim}_*(M_1, M_2) \models x \approx x'$, making $\neg\mathsf{alloc}(x)$ actually redundant. Consequently, equivalence is preserved when only the literals $\neg\mathsf{alloc}(x) \in M_1 \cup M_2$ are included in $\mathsf{elim}_*(M_1, M_2)$. This refined version of $\mathsf{elim}_*(M_1, M_2)$ is used in the proof of Lemma 6. However, taking this observation into account at this point would clutter the definition of $\mathsf{elim}_*(M_1, M_2)$. ■

Next, we prove a similar result for the separating implication. For technical convenience, we translate the septraction $M_1 \multimap M_2$, instead of $M_1 \twoheadrightarrow M_2$, as an equivalent boolean combination of test formulae. This is without loss of generality, because $M_1 \twoheadrightarrow M_2 \equiv \neg(M_1 \multimap \neg M_2)$. Unlike with the case of the separating conjuction (Lemma 3), here the definition of the boolean combination of test formulae depends on whether the universe is finite or infinite.

If the complement of some literal $\ell \in \mathsf{fp}_a(M_1)$ belongs to M_2 then no extension by a heap that satisfies ℓ may satisfy $\neg\ell$. Therefore, as an additional simplifying assumption, we suppose that $\mathsf{fp}_a(M_1) \cap \overline{M_2} = \emptyset$, so that $M_1 \multimap M_2$ is not trivially unsatisfiable.

Lemma 4. *Let M_1 and M_2 be two footprint-consistent minterms that are E-complete for $\mathsf{var}(M_1 \cup M_2)$, such that (a) M_1 is A-complete for $\mathsf{var}(M_1 \cup M_2)$, (b) $M_2^a \cup M_2^p \subseteq \mathsf{cc}(M_1^a \cup M_1^p)$, and (c) $\mathsf{fp}_a(M_1) \cap \overline{M_2} = \emptyset$. Then, we have:*

$$M_1 \multimap M_2 \equiv^{fin} \mathsf{elim}^{fin}_{\multimap}(M_1, M_2)$$
$$M_1 \multimap M_2 \equiv^{inf} \mathsf{elim}^{inf}_{\multimap}(M_1, M_2)$$

where $\mathsf{elim}^{\dagger}_{\multimap}(M_1, M_2)$, for $\dagger \in \{fin, inf\}$ is defined as:

$$\mathsf{pc}(M_1)^e \wedge M_2^e \wedge \mathsf{dc}(M_1)^u \wedge \mathsf{dc}(M_2)^u \wedge \quad (11)$$
$$\mathsf{nalloc}(\mathsf{av}(M_1)) \wedge \mathsf{fp}_{\mathsf{nv}(M_1)}(M_2) \wedge \quad (12)$$
$$|h| \geq \min_{M_2} - \max_{M_1} + 1 \wedge |h| < \max_{M_2} - \min_{M_1} \quad (13)$$
$$\wedge\ \lambda^{\dagger} \quad (14)$$

where $\lambda^{inf} \stackrel{\text{def}}{=} \top$ *and* $\lambda^{fin} \stackrel{\text{def}}{=}$

$$\bigwedge_{Y \subseteq \mathsf{var}(M_1 \cup M_2)} \mathsf{nalloc}(Y) \rightarrow \begin{pmatrix} |h| < |U| - \min_{M_1} - \#_n(Y, M_1) + 1 \\ \wedge\ |U| \geq \min_{M_2} + \#_n(Y, M_1) \end{pmatrix}$$

Observe that a heap satisfies $M_1 \multimap M_2$ iff it has an extension, by a disjoint heap satisfying M_1, that satisfies M_2. Thus, $\mathsf{elim}^{\dagger}_{\multimap}(M_1, M_2)$ must entail the heap-independent literals of both M_1 and M_2 (11). Next, no variable allocated by M_1 must be allocated by $\mathsf{elim}^{\dagger}_{\multimap}(M_1, M_2)$, otherwise no extension with a heap satisfying M_1 is possible and, moreover, the footprint of M_2 relative to the unallocated variables of M_1 must be asserted (12). The heap's cardinality constraints depend on the bounds of M_1 and M_2 (13) and, if Y is a set of variables not allocated in the heap, these variables might occur allocated in the extension (14).

Actually, this is where the finite universe assumption first comes into play. If the universe is infinite, then there are enough many locations outside the heap to be assigned to Y. However, if the universe is finite, then it is necessary to ensure that there are at least $\#_n(Y, M_1)$ free locations to be assigned to Y (14). Note that $\mathsf{elim}^{fin}_{\multimap}(M_1, M_2)$ introduces positive $\mathsf{alloc}(x)$ test formulae (remark 1), in the definition of λ^{fin} (14). These formulae do not match the polarity of the separating implication $M_1 \twoheadrightarrow M_2 = \neg(M_1 \multimap \neg M_2)$.

Proof: If $\mathsf{pc}(M_1) = \bot$ then $M_1 \multimap M_2 \equiv \mathsf{elim}_{\multimap}(M_1, M_2) \equiv \bot$. Also, since M_1 and M_2 are E-complete for $\mathsf{var}(M_1 \cup M_2)$, if we suppose that $M_1^e \neq M_2^e$ then $M_1 \multimap M_2 \equiv \mathsf{elim}_{\multimap}(M_1, M_2) \equiv \bot$. From now on, we shall assume that $\mathsf{pc}(M_1) = M_1$ and $M_1^e = M_2^e$.

$\boxed{M_1 \multimap M_2 \models \mathsf{elim}_{\multimap}(M_1, M_2)}$ Let $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ be a structure such that $\mathcal{I} \models M_1 \multimap M_2$. Then there exists a heap $\mathfrak{h}'$ disjoint from $\mathfrak{h}$ such that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models M_1$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus \mathfrak{h}') \models M_2$. Below we prove that $\mathcal{I}$ is also a model of the formulae (11), (12), (13) and (14), respectively.

(11) We have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models M_1^e \wedge M_1^u$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models M_1^e \wedge M_1^u$ by Proposition 5, and by Proposition 7, we deduce that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{pc}(M_1)^e \wedge \mathsf{dc}(M_1)^u$. Analogously, $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models M_2^e \wedge \mathsf{dc}(M_2)^u$ follows from $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus \mathfrak{h}') \models M_2$ by Propositions 5 and 7.

(12) Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models M_1$, also $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models \mathsf{alloc}(\mathsf{av}(M_1))$ and since $\mathrm{dom}(\mathfrak{h}') \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{nalloc}(\mathsf{av}(M_1))$. To prove that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{fp}_{\mathsf{nv}(M_1)}(M_2)$, we consider four cases, depending on the form of the literal:

- If $\mathsf{alloc}(x) \in M_2$ and $x \in \mathsf{nv}(M_1)$, then $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h}) \cup \mathrm{dom}(\mathfrak{h}')$ and $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h}')$, thus $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h})$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{alloc}(x)$, by Proposition 1.
- The case $x \hookrightarrow \mathbf{y} \in M_2$ and $x \in \mathsf{nv}(M_1)$ uses a similar argument.
- If $\neg\mathsf{alloc}(x) \in M_2$ and $x \in \mathsf{nv}(M_1)$, then $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h} \cup \mathfrak{h}')$, hence $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h})$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg\mathsf{alloc}(x)$, by Proposition 1.
- If $\neg x \hookrightarrow \mathbf{y} \in M_2$ and $x \in \mathsf{nv}(M_1)$ then $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h}')$ and either:

- $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h})$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg x \hookrightarrow \mathbf{y}$, by Proposition 1, or
- $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h})$ in which case $\mathfrak{h}' \uplus \mathfrak{h}$ and $\mathfrak{h}$ agree on $\mathfrak{s}(x)$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \neg x \hookrightarrow \mathbf{y}$.

(13) We have $||\mathfrak{h} \uplus \mathfrak{h}'|| = ||\mathfrak{h}|| + ||\mathfrak{h}'||$ and since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus \mathfrak{h}') \models M_2$, we obtain $\min^{\mathcal{I}}_{M_2} \leq ||\mathfrak{h}|| + ||\mathfrak{h}'|| < \max^{\mathcal{I}}_{M_2}$. Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models M_1$ we also have $\min^{\mathcal{I}}_{M_1} \leq ||\mathfrak{h}'|| < \max^{\mathcal{I}}_{M_1}$, thus $\min^{\mathcal{I}}_{M_1} \leq ||\mathfrak{h}'|| \leq \max^{\mathcal{I}}_{M_1} - 1$, i.e., $-\max^{\mathcal{I}}_{M_1} + 1 \leq -||\mathfrak{h}'|| \leq -\min^{\mathcal{I}}_{M_1}$ so that $\min^{\mathcal{I}}_{M_2} - \max^{\mathcal{I}}_{M_1} + 1 \leq ||\mathfrak{h}|| < \max^{\mathcal{I}}_{M_2} - \min^{\mathcal{I}}_{M_1}$.

(14) Assume that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{nalloc}(Y)$ for a set $Y \subseteq \mathsf{var}(M_1 \cup M_2)$, which implies that $\mathrm{dom}(\mathfrak{h}) \cap \mathfrak{s}(Y) = \emptyset$. Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models M_1$, we also have $\mathrm{dom}(\mathfrak{h}') \cap \mathfrak{s}(\mathsf{nv}(M_1)) = \emptyset$. Thus $||\mathfrak{U}|| \geq ||\mathfrak{h}|| + ||\mathfrak{h}'|| + ||\mathfrak{s}(Y \cap \mathsf{nv}(M_1))|| \geq ||\mathfrak{h}|| + \min^{\mathcal{I}}_{M_1} + \#_n(Y, M_1)$, because $||\mathfrak{h}'|| \geq \min^{\mathcal{I}}_{M_1}$ and $||\mathfrak{s}(Y \cap \mathsf{nv}(M_1))|| = |Y \cap \mathsf{nv}(M_1)|_{M_1} = \#_n(Y, M_1)$, by Proposition 6, since M_1 is E-complete. Therefore, $||\mathfrak{h}|| \leq ||\mathfrak{U}|| - \min^{\mathcal{I}}_{M_1} - \#_n(Y, M_1)$. Moreover, since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus \mathfrak{h}') \models M_2$, we obtain $|U| \geq ||\mathfrak{h} \uplus \mathfrak{h}'|| + \#_n(Y, M_1) \geq \min^{\mathcal{I}}_{M_2} + \#_n(Y, M_1)$.

$\boxed{\mathsf{elim}_{-\circ}(M_1, M_2) \models M_1 -\!\!\circ\, M_2}$ Let $\mathcal{I} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ be a structure such that $\mathcal{I} \models \mathsf{elim}_{-\circ}(M_1, M_2)$. We shall build a heap $\mathfrak{h}'$ such that $\mathrm{dom}(\mathfrak{h}) \cap \mathrm{dom}(\mathfrak{h}') = \emptyset$, $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models M_1$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus \mathfrak{h}') \models M_2$. First, for each variable $x \in \mathsf{av}(M_1)$ such that $x' \hookrightarrow \mathbf{y} \in M_1^p$ for some variable x' with $x \approx_{M_1} x'$, we add the tuple $(\mathfrak{s}(x), \mathfrak{s}(\mathbf{y}))$ to $\mathfrak{h}'$. Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{pc}(M_1)^e$, for any pair of variables $x \approx_{M_1} x'$ if $x \hookrightarrow \mathbf{y}, x' \hookrightarrow \mathbf{y}' \in M_1$ then $y_i \approx_{M_1} y'_i$, and the result is a functional relation. We define:

$$
\begin{aligned}
A &= \{x \in \mathsf{av}(M_1) \mid \forall x' \forall \mathbf{y} \,.\, x \approx_{M_1} x' \Rightarrow x' \hookrightarrow \mathbf{y} \notin M_1^p\} \\
V_x &= \{(\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k)) \in \mathfrak{U}^k \mid x \approx_{M_1} x',\ \neg x' \hookrightarrow \mathbf{y} \in M_1^p\},\ \text{for } x \in \mathsf{av}(M_1) \\
N &= \{x \in \mathsf{var}(M_1 \cup M_2) \mid \mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h})\}
\end{aligned}
$$

Intuitively, A denotes the set of variables that must be allocated but with no constraint on their image; this set is independent of the interpretation under consideration. The set V_x denotes the set of images the allocated variable x cannot point to, and N denotes the set of variables that are not allocated in $\mathfrak{h}$.

Then for each $x \in A$ we choose a tuple $(\ell_1, \ldots, \ell_k) \in \mathfrak{U}^k \setminus V_x$ and let $\mathfrak{h}'(\mathfrak{s}(x)) = (\ell_1, \ldots, \ell_k)$. Since M_1 is E-complete, we have $||V_x|| \leq \delta_x(M_1)$ for each $x \in A$, and such a choice is possible because $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{dc}(M_1)^u$, thus $||\mathfrak{U}^k|| \geq \delta_x(M_1) + 1$.

Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{nalloc}(N)$, if $\mathfrak{U}$ is finite, by (13) it must be the case that:

$$
||\mathfrak{h}|| < ||\mathfrak{U}|| - \min^{\mathcal{I}}_{M_1} - \#_n(N, M_1) + 1 \tag{15}
$$

$$
||\mathfrak{U}|| \geq \min^{\mathcal{I}}_{M_2} + \#_n(N, M_1) \tag{16}
$$

Finally, let $L \subseteq \mathfrak{U} \setminus (\mathrm{dom}(\mathfrak{h}) \cup \mathfrak{s}(\mathsf{av}(M_1)) \cup \mathfrak{s}(\mathsf{nv}(M_1)))$ be a finite set of locations of cardinality $||L|| = \max(\min^{\mathcal{I}}_{M_1}, \min^{\mathcal{I}}_{M_2} - ||\mathfrak{h}||) - \#_a(M_1)$. Choosing such a set L

is possible, because either $\mathfrak{U}$ is infinite, or $\mathfrak{U}$ is finite, in which case:

$$\begin{aligned}
||\mathfrak{U}|| &\geq \max(\min^{\mathcal{I}}_{M_1} + ||\mathfrak{h}||, \min^{\mathcal{I}}_{M_2}) + \#_n(N, M_1), \text{ by (15) and (16)} \\
&\geq \max(\min^{\mathcal{I}}_{M_1}, \min^{\mathcal{I}}_{M_2} - ||\mathfrak{h}||) - \#_a(M_1) + ||\mathfrak{h}|| + \#_a(M_1) + \#_n(N, M_1) \\
&= ||L|| + ||\mathfrak{h}|| + \#_a(M_1) + \#_n(N, M_1) \\
&\geq ||L|| + ||\mathrm{dom}(h) \cup \mathfrak{s}(\mathsf{av}(M_1)) \cup \mathfrak{s}(\mathsf{nv}(M_1))||
\end{aligned}$$

where the last inequality is a consequence of Proposition 6. We choose an arbitrary tuple $(\ell_1, \ldots, \ell_k) \in \mathfrak{U}^k$ and let $\mathfrak{h}'(\ell) = (\ell_1, \ldots, \ell_k)$ for all $\ell \in L$. Because $\mathfrak{U}$ is non-empty, such a tuple exists. Consequently, we have $\mathrm{dom}(\mathfrak{h}') = \mathfrak{s}(\mathsf{av}(M_1)) \cup L$ and $\mathrm{dom}(\mathfrak{h}') \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$ because $\mathfrak{s}(\mathsf{av}(M_1)) \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$ by (12) and $L \cap \mathrm{dom}(\mathfrak{h}) = \emptyset$ by construction. We now prove:

$(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models M_1$. Clearly $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models M_1^e \wedge M_1^u$ by (11) and Proposition 7. To show $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models M_1^a$, observe that $\mathfrak{s}(x) \in \mathrm{dom}(\mathfrak{h}')$ for each $x \in \mathsf{av}(M_1)$, hence for each literal $\mathsf{alloc}(x) \in M_1$ we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models \mathsf{alloc}(x)$. Moreover, we have $\mathrm{dom}(\mathfrak{h}') \cap \mathfrak{s}(\mathsf{nv}(M_1)) = (\mathfrak{s}(\mathsf{av}(M_1)) \cup L) \cap \mathfrak{s}(\mathsf{nv}(M_1)) = \emptyset$, because M_1 is footprint consistent and E-complete for $\mathsf{var}(M_1 \cup M_2)$, by Proposition 9. Thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models \neg\mathsf{alloc}(x)$ for each literal $\neg\mathsf{alloc}(x) \in M_1^a$. For each literal $x \hookrightarrow \mathbf{y} \in M_1^p$ we have $\mathfrak{h}'(\mathfrak{s}(x)) = (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))$ by construction, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models x \hookrightarrow \mathbf{y}$. For each literal $\neg x \hookrightarrow \mathbf{y} \in M_1^p$, we distinguish two cases.

- If $x \in \mathsf{av}(M_1)$, then $(\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k)) \in V_x$ hence $\mathfrak{h}(\mathfrak{s}(x)) \neq (\mathfrak{s}(y_1), \ldots, \mathfrak{s}(y_k))$ by construction.
- If $x \notin \mathsf{av}(M_1)$, then since M_1 is A-complete for $\mathsf{var}(M_1 \cup M_2)$, we have $x \in \mathsf{nv}(M_1)$, thus $\mathfrak{s}(x) \notin \mathrm{dom}(\mathfrak{h}') = \mathfrak{s}(\mathsf{av}(M_1)) \cup L$.

We finally prove that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models |h| \geq \min_{M_1} \wedge |h| < \max_{M_1}$. Since $\mathrm{dom}(\mathfrak{h}') = \mathfrak{s}(\mathsf{av}(M_1)) \cup L$ and $\mathfrak{s}(\mathsf{av}(M_1)) \cap L = \emptyset$, we have $||\mathfrak{h}'|| = ||\mathfrak{s}(\mathsf{av}(M_1))|| + ||L|| = \max(\min^{\mathcal{I}}_{M_1}, \min^{\mathcal{I}}_{M_2} - ||\mathfrak{h}||)$. If $||\mathfrak{h}'|| = \min^{I}_{M_1}$ then $||\mathfrak{h}'|| < \max^{I}_{M_1}$ because $\mathcal{I} \models \mathsf{dc}(M_1)^u$, which implies that $\min^{\mathcal{I}}_{M_1} < \max^{\mathcal{I}}_{M_1}$, by Proposition 8. Otherwise $||\mathfrak{h}'|| = \min^{\mathcal{I}}_{M_2} - ||\mathfrak{h}|| \geq \min^{I}_{M_1}$ and we have by (13) $||\mathfrak{h}|| \geq \min^{I}_{M_2} - \max^{I}_{M_1} + 1$, thus $||\mathfrak{h}|| > \min^{I}_{M_2} - \max^{I}_{M_1}$, and therefore $||\mathfrak{h}'|| < \max^{I}_{M_1}$.

$(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}' \uplus \mathfrak{h}) \models M_2$. We have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}' \uplus \mathfrak{h}) \models M_2^e \wedge M_2^u$ because $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models M_2^e \wedge M_2^u$ and these formulae do not depend on the heap. Next, for a given variable x, let $\alpha_x \in \{\mathsf{alloc}(x), \neg\mathsf{alloc}(x), x \hookrightarrow \mathbf{y}, \neg x \hookrightarrow \mathbf{y} \mid \mathbf{y} \in \mathsf{Var}^k\} \cap M_2$ be a literal and let $\overline{\alpha}_x$ denote its complement. If $x \in \mathsf{nv}(M_1)$ then $\alpha_x \in \mathsf{fp}_{\mathsf{nv}(M_1)}(M_2)$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \alpha_x$ by (12). Moreover, because $\mathfrak{h}$ and $\mathfrak{h} \uplus \mathfrak{h}'$ agree on $\mathfrak{s}(\mathsf{nv}(M_1))$, we obtain $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus \mathfrak{h}') \models \alpha_x$. Otherwise $x \notin \mathsf{nv}(M_1)$ hence $x \in \mathsf{av}(M_1)$ because M_1 is A-complete for $\mathsf{var}(M_1 \cup M_2)$, and since $\alpha_x \in M_2^a \cup M_2^p \subseteq \mathsf{cc}(M_1^a \cup M_1^p)$, we have $\alpha_x \in \mathsf{fp}_a(M_1)$, because the case $\overline{\alpha}_x \in \mathsf{fp}_a(M_1)$ is in contradiction with $\mathsf{fp}_a(M_1) \cap \overline{M_2} = \emptyset$ (condition (c) of the Lemma). But then $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}') \models \alpha_x$ and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus \mathfrak{h}') \models \alpha_x$ follows, by Proposition 3. We have thus proved that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h} \uplus$

$\mathfrak{h}') \models M_2^a \cup M_2^p$. We are left with proving that $\min_{M_2}^{\mathcal{I}} \leq \|\mathfrak{h}\| + \|\mathfrak{h}'\| = \max(\min_{M_1}^{\mathcal{I}} + \|\mathfrak{h}\|, \min_{M_2}^{\mathcal{I}}) < \max_{M_2}^{\mathcal{I}}$. If $\min_{M_1}^{\mathcal{I}} + \|\mathfrak{h}\| \leq \min_{M_2}^{\mathcal{I}}$ the result follows from the fact that $\mathcal{I} \models \mathsf{dc}(M_2)^u$, which implies $\min_{M_2}^{\mathcal{I}} < \max_{M_2}^{\mathcal{I}}$, by Proposition 8. Otherwise, $\|\mathfrak{h}\| + \|\mathfrak{h}'\| = \min_{M_1}^{\mathcal{I}} + \|\mathfrak{h}\| > \min_{M_2}^{\mathcal{I}}$ and $\|\mathfrak{h}\| + \|\mathfrak{h}'\| < \max_{M_2}^{\mathcal{I}}$ follows from (13). □

4.2 Translating Quantifier-free SL^k into Minterms

We prove next that each quantifier-free SL^k formula is equivalent to a finite disjunction of minterms. Given minterms M_1 and M_2, we define:

$$\mathrm{minh}(M_1, M_2) \stackrel{\mathsf{def}}{=} \begin{cases} \{|h| \geq \max(\min_{M_1}, \min_{M_2})\} \\ \quad \text{if } \min_{M_1}, \min_{M_2} \in \mathbb{N} \\ \left\{ \begin{array}{l} |h| \geq \min_{M_i} \wedge |U| < \min_{M_i} + m + 1, \\ |h| \geq \min_{M_{3-i}} \wedge |U| \geq \min_{M_i} + m + 1 \end{array} \right\} \\ \quad \text{if } \min_{M_i} \in \mathbb{N}, \min_{M_{3-i}} = |U| - m, i = 1, 2 \\ \{|h| \geq |U| - \min(m_1, m_2)\} \\ \quad \text{if } \min_{M_i} = |U| - m_i, i = 1, 2 \end{cases}$$

$$\mathrm{maxh}(M_1, M_2) \stackrel{\mathsf{def}}{=} \begin{cases} \{|h| < \min(\max_{M_1}, \max_{M_2})\} \\ \quad \text{if } \max_{M_1}, \max_{M_2} \in \mathbb{N}_\infty \\ \{|h| < \max_{M_i}\} \\ \quad \text{if } \max_{M_{3-i}} = \infty, \max_{M_i} = |U| - m, i = 1, 2 \\ \left\{ \begin{array}{l} |h| < \max_{M_i} \wedge |U| \geq \max_{M_i} + m, \\ |h| < |U| - m \wedge |U| < \max_{M_i} + m \end{array} \right\} \\ \quad \text{if } \max_{M_i} \in \mathbb{N}, \max_{M_{3-i}} = |U| - m, i = 1, 2 \\ \{|h| < |U| - \max(m_1, m_2)\} \\ \quad \text{if } \max_{M_i} = |U| - m_i, i = 1, 2 \end{cases}$$

Intuitively, we merge the cardinality constraints occurring in M_1 and M_2, by taking the conjunction and keeping only the most restrictive bounds. For instance, if $M_1 = \{|h| \geq 2, |h| < |U| - 1\}$ and $M_2 = \{|h| \geq 3, |h| < |U| - 2\}$, then $\mathrm{minh}(M_1, M_2) = \{|h| \geq 3\}$ and $\mathrm{maxh}(M_1, M_2) = \{|h| < |U| - 2\}$. Heterogeneous constraints are merged by performing a case split on the value of $|U|$, which explains why $\mathrm{minh}(M_1, M_2)$ is a set of conjunctions, and not a single conjunction. For example, if $M_1' = \{|h| \geq |U| - 4\}$ and $M_2' = \{|h| \geq 1\}$, then the first condition prevails if $|U| \geq 5$ yielding: $\mathrm{minh}(M_1', M_2') = \{|h| \geq 1 \wedge |U| < 5, |h| \geq |U| - 4 \wedge |U| \geq 5\}$. The disjunction of minterms equivalent to a conjunction of two minterms is then defined as: $[M_1, M_2] \stackrel{\text{def}}{=}$

$$\{ \bigwedge_{i=1,2} M_i^e \wedge M_i^a \wedge M_i^p \wedge M_i^u \wedge \mu \wedge \nu \mid \mu \in \mathrm{minh}(M_1, M_2), \\ \nu \in \mathrm{maxh}(M_1, M_2)\}$$

We extend this notation recursively to any set of minterms of size $n > 2$, as $[M_1, M_2, \ldots, M_n] \stackrel{\text{def}}{=} \bigcup_{M \in [M_1,\ldots,M_{n-1}]} [M, M_n]$.

Proposition 10. *Given minterms $M_1, \ldots, M_n$, we have $\bigwedge_{i=1}^n M_i \equiv \bigvee_{M \in [M_1,\ldots,M_n]} M$.*

Proof: We prove the result for $n = 2$, the general result follows by induction. For $n = 2$, this is a consequence of the fact that $|h| \geq \min_{M_1} \wedge |h| \geq \min_{M_2} \equiv \bigvee_{\mu \in \mathrm{minh}(M_1,M_2)} \mu$, and $|h| < \max_{M_1} \wedge |h| < \max_{M_2} \equiv \bigvee_{\nu \in \mathrm{maxh}(M_1,M_2)} \nu$. We prove the first fact in the case where $\min_{M_1} = m_1$ and $\min_{M_2} = |U| - m_2$, the other cases are similar. Consider a structure $\mathcal{I} = (\mathfrak{U}, \mathfrak{h}, \mathfrak{s})$ such that $\mathcal{I} \models |h| \geq m_1 \wedge |h| \geq |U| - m_2$. Then $||\mathfrak{h}|| \geq m_1$ and $||\mathfrak{h}|| \geq ||\mathfrak{U}|| - m_2$, and we distinguish two cases.

- if $m_1 \geq ||U|| - m_2$, then necessarily $||\mathfrak{U}|| < m_1 + m_2 + 1$, so that $\mathcal{I} \models |h| \geq m_1 \wedge |U| < m_1 + m_2 + 1$.
- otherwise, we have $||U|| \geq m_1 + m_2 + 1$, so that $\mathcal{I} \models |h| \geq |U| - m_2 \wedge |U| \geq m_1 + m_2 + 1$.

Conversely, if $\mathcal{I}$ is a structure such that either $\mathcal{I} \models |h| \geq m_1 \wedge |U| < m_1 + m_2 + 1$ or $\mathcal{I} \models |h| \geq |U| - m_2 \wedge |U| \geq m_1 + m_2 + 1$, then it is straightforward to verify that $\mathcal{I} \models |h| \geq m_1 \wedge |h| \geq |U| - m_2$. $\square$

Proposition 11. *Given minterms $M_1, \ldots, M_n$ and $M \in [M_1, \ldots, M_n]$, if $\ell \in M$ is a literal then either $\ell \in M_i$, for some $i = 1, \ldots, n$, or $\ell \in \{|U| \geq m_1 + m_2, |U| < m_1 + m_2, |U| \geq m_1 + m_2 + 1, |U| < m_1 + m_2 + 1\}$, where $M_1 \cup \cdots \cup M_n$ contains two literals $\ell_i \in \{|h| \geq m_i, |h| < m_i, |h| \geq |U| - m_i, |h| < |U| - m_i\}$, for $i = 1, 2$.*

Proof: Assume that $n = 2$. If $\ell \notin M_1 \cup M_2$ then by definition of $[M_1, M_2]$, necessarily ℓ occurs in $\mathrm{minh}(M_1, M_2) \cup \mathrm{maxh}(M_1, M_2)$ and the proof is immediate, by definition of these sets. The proof for $n > 2$ goes by induction on n. $\square$

Given a set L of literals and a subset $B \subseteq L$, let $L^B \stackrel{\text{def}}{=} B \cup \{\overline{\ell} \mid \ell \in L \setminus B\}$. For a set K of literals, let $(K)^L \stackrel{\text{def}}{=} \{K \cup L^B \mid B \subseteq L\}$ be the set of completions of K using literals from L and their complements, so that $K \subseteq (K)^L$ and $(K)^L$ contains either ℓ or $\overline{\ell}$, for every $\ell \in L$.

Proposition 12. *If K and L are sets of literals, then $K \equiv \bigvee_{\psi \in (K)^L} \psi$. If further K is a minterm and L contains no literals of the form $|h| \geq t$ or $|h| < t$, then every set $P \in (K)^L$ is a minterm such that* $\mathsf{var}(P) = \mathsf{var}(K) \cup \mathsf{var}(L)$, $\min_P = \min_K$ *and* $\max_P = \max_K$.

Proof: Immediate, by the definition of $(K)^L$. □

For a literal ℓ, let $[\ell]^{\mathsf{mt}}$ be an equivalent minterm obtained from ℓ by adding the missing lower/upper bounds on the cardinality of the heap, namely $|h| \geq 0$ if $\ell \notin \{|h| \geq n, |h| \geq |U| - n \mid n \in \mathbb{Z}\}$ and $|h| < \infty$ if $\ell \notin \{|h| < n, |h| < |U| - n \mid n \in \mathbb{Z}\}$. We extend this notation to sets of literals as $[\ell_1, \ldots, \ell_n]^{\mathsf{mt}} \stackrel{\mathsf{def}}{=} [[\ell_1]^{\mathsf{mt}}, \ldots, [\ell_n]^{\mathsf{mt}}]$. We have $\ell \equiv [\ell]^{\mathsf{mt}}$ for any literal ℓ and $L \equiv \bigvee_{M \in [L]^{\mathsf{mt}}} M$, for any set L of literals. For a boolean combination of literals ϕ, we denote by $(\phi)^{\mathsf{dnf}}$ its disjunctive normal form. Given a formula ϕ in disjunctive normal form $\phi = \bigvee_{i=1}^n L_i$, where each conjunctive clause L_i is identified with the set of its elements, we define $[\phi]^{\mathsf{mt}} \stackrel{\mathsf{def}}{=} \bigcup_{i=1}^n [L_i]^{\mathsf{mt}}$. We have $[\phi]^{\mathsf{mt}} \equiv \bigvee_{M \in [\phi]^{\mathsf{mt}}} M$. Further, let $\mathsf{E}(L) \stackrel{\mathsf{def}}{=} \{x \approx y \mid x, y \in \mathsf{var}(L)\}$ and $\mathsf{A}(L) \stackrel{\mathsf{def}}{=} \{\mathsf{alloc}(x) \mid x \in \mathsf{var}(L)\}$, for a set L of literals.

For each $\dagger \in \{\mathit{fin}, \mathit{inf}\}$, we define the set of minterms $\mu^\dagger(\phi)$ recursively on the structure of ϕ, as follows:

$$
\begin{aligned}
\mu^\dagger(\mathsf{emp}) &\stackrel{\mathsf{def}}{=} \{|h| \approx 0\} \\
\mu^\dagger(x \mapsto \mathbf{y}) &\stackrel{\mathsf{def}}{=} \{x \hookrightarrow \mathbf{y} \wedge |h| \approx 1\} \\
\mu^\dagger(x \approx y) &\stackrel{\mathsf{def}}{=} \{x \approx y \wedge |h| \geq 0 \wedge |h| < \infty\} \\
\mu^\dagger(\phi_1 \wedge \phi_2) &\stackrel{\mathsf{def}}{=} \bigcup_{\substack{M_i \in \mu^\dagger(\phi_i) \\ i=1,2}} [M_1, M_2] \\
\mu^\dagger(\neg\phi_1) &\stackrel{\mathsf{def}}{=} \bigcup \left\{ \left[\overline{\ell_1}, \ldots, \overline{\ell_n}\right]^{\mathsf{mt}} \middle| \ell_i \in M_i,\ i \in [1,n] \right\} \\
&\quad \text{where } \mu^\dagger(\phi_1) = \{M_1, \ldots, M_n\}
\end{aligned}
$$

$$
\begin{aligned}
&\mu^\dagger(\phi_1 * \phi_2) \stackrel{\mathsf{def}}{=} \\
&\bigcup_{\substack{M_i \in \mu^\dagger(\phi_i) \\ i=1,2}} \left\{ [(\mathsf{elim}_*(P_1, P_2))^{\mathsf{dnf}}]^{\mathsf{mt}} \middle| \begin{array}{l} N_j \in (M_j)^{\mathsf{E}(M_1 \cup M_2)}, \\ P_j \in (N_j)^{N^p_{3-j}}, j = 1,2 \end{array} \right\}
\end{aligned}
$$

$$
\begin{aligned}
&\mu^\dagger(\phi_1 \multimap \phi_2) \stackrel{\mathsf{def}}{=} \\
&\bigcup_{\substack{M_i \in \mu^\dagger(\phi_i) \\ i=1,2}} \left\{ \left[(\mathsf{elim}^\dagger_{\multimap}(Q_1, N_2))^{\mathsf{dnf}}\right]^{\mathsf{mt}} \middle| \begin{array}{l} N_j \in (M_j)^{\mathsf{E}(M_1 \cup M_2)}, \\ P_1 \in (N_1)^{\mathsf{A}(M_1 \cup M_2)}, \\ Q_1 \in (P_1)^{M_2^a \cup M_2^p}, j = 1,2 \end{array} \right\}
\end{aligned}
$$

Intuitively, $\mu^\dagger(\phi_1 * \phi_2)$ and $\mu^\dagger(\phi_1 \multimap \phi_2)$ are computed by first computing recursively $\mu^\dagger(\phi_1)$ and $\mu^\dagger(\phi_2)$, then extending the obtained minterms in such a way that the hypotheses of Lemmas 3 or 4 are satisfied, and finally applying $\mathsf{elim}^\dagger_*$ and $\mathsf{elim}^\dagger_{\multimap}$, respectively.

Example 1. For instance, consider the formula $x \mapsto x \multimap y \mapsto y$. It is easy to check that $\mu^\dagger(x \hookrightarrow x) = \{M_1\}$, where $M_1 = x \hookrightarrow x \wedge |h| \geq 1 \wedge |h| < 2$ and

$\mu^\dagger(y \mapsto y) = \{M_2\}$, where $M_2 = y \hookrightarrow y \wedge |h| \geq 1 \wedge |h| < 2$. To apply Lemma 4, we need to ensure that M_1 and M_2 are E-complete, which may be done by adding either $x \approx y$ or $x \not\approx y$ to each minterm. We also have to ensure that M_1 is A-complete, thus we add either $\mathsf{alloc}(z)$ or $\neg\mathsf{alloc}(z)$ to M_1, for $z \in \{x, y\}$. Finally, we must have $M_2^a \cup M_2^p \subseteq \mathsf{cc}(M_1^a \cup M_1^p)$, thus we add either $x \hookrightarrow x$ or $\neg x \hookrightarrow x$ into M_1. After removing redundancies, we get (among others) the minterms: $M_1' = x \hookrightarrow x \wedge |h| \geq 1 \wedge |h| < 2 \wedge x \approx y$ and $M_2' = y \hookrightarrow y \wedge |h| \geq 1 \wedge |h| < 2 \wedge x \approx y$. Afterwards we compute $\mathsf{elim}^{\mathit{fin}}_{-\!\circ}(M_1', M_2') = x \approx y \wedge \neg\mathsf{alloc}(x) \wedge |h| \geq 0 \wedge |h| < 1$. ■

Lemma 5. *Given a quantifier-free* SL^k *formula* ϕ*, the following equivalences hold: (1)* $\phi \equiv^{\mathit{fin}} \bigvee_{M \in \mu^{\mathit{fin}}(\phi)} M$*, and (2)* $\phi \equiv^{\mathit{inf}} \bigvee_{M \in \mu^{\mathit{inf}}(\phi)} M$*.*

Proof: (1) We show that $\phi \equiv^{\mathit{fin}} \bigvee_{M \in \mu^{\mathit{fin}}(\phi)} M$ by induction on the structure of ϕ. The base cases are immediate and the inductive cases are dealt with below:

- if $\phi = \phi_1 \wedge \phi_2$ and $\phi_i \equiv^{\mathit{fin}} \bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i)} M_i$ for $i = 1, 2$ by the inductive hypothesis and Proposition 10, we have:

$$\begin{aligned}\phi &\equiv^{\mathit{fin}} \bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i),\ i=1,2} M_1 \wedge M_2 \\ &\equiv^{\mathit{fin}} \bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i),\ i=1,2} \bigvee_{M \in [M_1, M_2]} M\end{aligned}$$

- if $\phi = \neg\phi_1$, $\mu^{\mathit{fin}}(\phi_1) = \{M_1, \ldots, M_n\}$, $M_i = \{\ell_{i1}, \ldots, \ell_{in_i}\}$ for all $i \in [1, n]$, then since $\phi_1 \equiv^{\mathit{fin}} \bigvee_{i=1}^{n} \bigwedge_{j=1}^{n_i} \ell_{ij}$ by the inductive hypothesis, we have:

$$\begin{aligned}\neg\phi_1 &\equiv^{\mathit{fin}} \bigwedge_{i=1}^{n} \bigvee_{j=1}^{n_i} \overline{\ell_{ij}} \\ &\equiv^{\mathit{fin}} \bigwedge_{i=1}^{n} \bigvee_{j=1}^{n_i} \left[\overline{\ell_{ij}}\right]^{\mathsf{mt}} \\ &\equiv^{\mathit{fin}} \bigvee \left\{ \left[\overline{\ell_1}\right]^{\mathsf{mt}} \wedge \ldots \wedge \left[\overline{\ell_n}\right]^{\mathsf{mt}} \,\middle|\, \ell_i \in M_i,\ i \in [1, n] \right\} \\ &\equiv^{\mathit{fin}} \bigvee \left\{ \left[\overline{\ell_1}, \ldots, \overline{\ell_n}\right]^{\mathsf{mt}} \,\middle|\, \ell_i \in M_i,\ i \in [1, n] \right\}\end{aligned}$$

- if $\phi = \phi_1 * \phi_2$ and $\phi_i \equiv^{\mathit{fin}} \bigvee_{M \in \mu^{\mathit{fin}}(\phi_i)} M$ for $i = 1, 2$ by the induction hypothesis, we compute successively[8]:

$$\begin{aligned}&(\phi_1 * \phi_2) \text{ [distributivity of } * \text{ with } \vee] \\ \equiv^{\mathit{fin}} &\bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i),\ i=1,2} M_1 * M_2 \\ &\left[\text{because } M_i \equiv \bigvee_{N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}} N_i\right] \\ \equiv^{\mathit{fin}} &\bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i),\ i=1,2} \bigvee_{N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}} N_1 * N_2 \\ &\left[\text{because } N_i \equiv \bigvee_{P_i \in (N_i)^{N_{3-i}^p}} P_i\right] \\ \equiv^{\mathit{fin}} &\bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i),\ i=1,2} \bigvee_{N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}} \\ &\bigvee_{P_i \in (N_i)^{N_{3-i}^p}} P_1 * P_2\end{aligned}$$

[8] See Definition 5 for the definition of N^p.

At this point, observe that N_i, and thus P_i, are E-complete for $\mathsf{var}(M_1 \cup M_2)$, for $i = 1, 2$. Moreover, $\mathsf{cc}(P_1^p) = \mathsf{cc}(P_2^p)$, because $P_i \in (N_i)^{N_{3-i}^p}$, for $i = 1, 2$. We can thus apply Lemma 3 and infer that:

$$\begin{aligned} P_1 * P_2 &\equiv \mathsf{elim}_*(P_1, P_2) \\ &\equiv (\mathsf{elim}_*(P_1, P_2))^{\mathsf{dnf}} \\ &\equiv \bigvee_{M \in \left[(\mathsf{elim}_*(P_1,P_2))^{\mathsf{dnf}}\right]^{\mathsf{mt}}} M \end{aligned}$$

– if $\phi = \phi_1 \multimap \phi_2$ and $\phi_i \equiv^{\mathit{fin}} \bigvee_{M \in \mu^{\mathit{fin}}(\phi_i)} M$, $i = 1, 2$, by the induction hypothesis, we compute, successively:

$$\begin{aligned} & (\phi_1 \multimap \phi_2)\,[\text{distributivity of } \multimap \text{ with } \vee] \\ \equiv^{\mathit{fin}} & \bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i),\ i=1,2} M_1 \multimap M_2 \\ & \left[\text{because } M_i \equiv \bigvee_{N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}} N_i\right] \\ \equiv^{\mathit{fin}} & \bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i),\ i=1,2} \bigvee_{N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}} N_1 \multimap N_2 \\ & \left[\text{because } N_1 \equiv \bigvee_{P_1 \in (N_1)^{\mathsf{A}(M_1 \cup M_2)}} P_1\right] \\ \equiv^{\mathit{fin}} & \bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i),\ i=1,2} \bigvee_{N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}} \\ & \bigvee_{P_1 \in (N_1)^{\mathsf{A}(M_1 \cup M_2)}} P_1 \multimap N_2 \\ & \left[\text{because } P_1 \equiv \bigvee_{Q_1 \in (P_1)^{N_2^a \cup N_2^p}} Q_1\right] \\ \equiv^{\mathit{fin}} & \bigvee_{M_i \in \mu^{\mathit{fin}}(\phi_i),\ i=1,2} \bigvee_{N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}} \\ & \bigvee_{P_1 \in (N_1)^{\mathsf{A}(M_1 \cup M_2)}} \bigvee_{Q_1 \in (P_1)^{N_2^a \cup N_2^p}} Q_1 \multimap N_2 \end{aligned}$$

Observe that N_i and thus P_i are E-complete for $\mathsf{var}(M_1 \cup M_2)$, for $i = 1, 2$. Moreover, P_1 is A-complete for $\mathsf{var}(M_1 \cup M_2)$, because $P_1 \in (N_1)^{\mathsf{A}(M_1 \cup M_2)}$ and $N_2^a \cup N_2^p \subseteq \mathsf{cc}(Q_1^a \cup Q_1^p)$, because $Q_1 \in (P_1)^{N_2^a \cup N_2^p}$. Then we can apply Lemma 4 and infer that:

$$\begin{aligned} Q_1 \multimap N_2 &\equiv^{\mathit{fin}} \mathsf{elim}_{\multimap}^{\mathit{fin}}(Q_1, N_2) \\ &\equiv \left(\mathsf{elim}_{\multimap}^{\mathit{fin}}(Q_1, N_2)\right)^{\mathsf{dnf}} \\ &\equiv \bigvee_{M \in \left[\left(\mathsf{elim}_{\multimap}^{\mathit{fin}}(Q_1,N_2)\right)^{\mathsf{dnf}}\right]^{\mathsf{mt}}} M \end{aligned}$$

(2) This point uses a similar argument. □

The following lemma relates the polarity of a test formula $|h| \geq |U| - n$ or $\mathsf{alloc}(x)$ that occur in some minterm $M \in \mu^{\mathit{fin}}(\phi) \cup \mu^{\mathit{inf}}(\phi)$ with that of a separating implication within ϕ (Remarks 1 and 2).

Lemma 6. *For any quantifier-free* SL^k *formula* ϕ*, we have:*

1. *For all* $M \in \mu^{\mathit{inf}}(\phi)$*, we have* $M \cap \{|h| \geq |U| - n, |h| < |U| - n \mid n \in \mathbb{N}\} = \emptyset$.
2. *If* $|h| \geq |U| - n \in M$ *[*$|h| < |U| - n \in M$*] for some minterm* $M \in \mu^{\mathit{fin}}(\phi)$*, then a formula* $\psi_1 \twoheadrightarrow \psi_2$ *occurs at a positive [negative] polarity in* ϕ.

3. *If* $\mathsf{alloc}(x) \in M$ *[*$\neg\mathsf{alloc}(x) \in M$*] for some minterm* $M \in \mu^{inf}(\phi)$*, then a formula* $\psi_1 \twoheadrightarrow \psi_2$*, such that* $x \in \mathsf{var}(\psi_1) \cup \mathsf{var}(\psi_2)$*, occurs at a positive [negative] polarity in* ϕ*.*
4. *If* $M \cap \{\mathsf{alloc}(x), \neg\mathsf{alloc}(x) \mid x \in \mathsf{Var}\} \neq \emptyset$ *for some minterm* $M \in \mu^{fin}(\phi)$*, then a formula* $\psi_1 \twoheadrightarrow \psi_2$*, such that* $x \in \mathsf{var}(\psi_1) \cup \mathsf{var}(\psi_2)$*, occurs in* ϕ *at some polarity* $p \in \{-1, 1\}$*. Moreover,* $\mathsf{alloc}(x)$ *occurs at a polarity* $-p$*, only if* $\mathsf{alloc}(x)$ *is in the scope of a* λ^{fin} *subformula (14) of a formula* $\mathsf{elim}^{fin}_{-\!\circ}(M_1, M_2)$ *used to compute* $\bigvee_{M \in \mu^{fin}(\phi)} M$*.*

Proof: (1) By induction on the structure of ϕ, one shows that no literal from $\{|h| \geq |U| - n, |h| < |U| - n \mid n \in \mathbb{N}\}$ is introduced during the construction of $\mu^{inf}(\phi)$. (2) Let $\ell \in M \cap \{|h| \geq |U| - n, |h| < |U| - n \mid n \in \mathbb{N}\}$ be a literal. The proof is by induction on the structure of ϕ:

- the cases $\phi = \mathsf{emp}$, $\phi = x \hookrightarrow \mathbf{y}$ and $\phi = x \approx y$ are trivial, because $\ell \notin \mu^{fin}(\phi)$.
- $\phi = \phi_1 \wedge \phi_2$: we have $M \in [M_1, M_2]$, for some minterms $M_i \in \mu^{fin}(\phi_i)$, for $i = 1, 2$. By Proposition 11, since $\ell \notin \{|U| \geq n, |U| < n \mid n \in \mathbb{N}\}$, we deduce that $\ell \in M_1 \cup M_2$ and the proof follows from the induction hypothesis, since any formula occurring in ϕ_i, $i = 1, 2$, occurs at the same polarity in ϕ.
- $\phi = \neg\phi_1$: assuming $\mu^{fin}(\phi_1) = \{M_1, \ldots, M_m\}$, we have $M \in \left[\overline{\ell_1}, \ldots, \overline{\ell_m}\right]^{\mathsf{mt}}$, for some literals $\ell_i \in M_i$, $i \in [1, m]$. By Proposition 11, we deduce that $\ell = \overline{\ell_i}$ for some $i = 1, \ldots, n$, because $\ell \notin \{|U| \geq n, |U| < n \mid n \in \mathbb{N}\}$. By the induction hypothesis, there exists a formula $\psi_1 \twoheadrightarrow \psi_2$ occurring at polarity $p \in \{1, -1\}$ in ϕ_1, where $p = 1$ if $\ell_i = |h| \geq |U| - n$ and $p = -1$ if $\ell_i = |h| < |U| - n$. Then ℓ occurs at polarity $-p$ in M and $\psi_1 \twoheadrightarrow \psi_2$ occurs at polarity $-p$ in ϕ.
- $\phi = \phi_1 * \phi_2$: for $i = 1, 2$, there exist minterms $M_i \in \mu^{fin}(\phi_i)$, $N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}$ and $P_i \in (N_i)^{N^p_{3-i}}$, such that $M \in \left[(\mathsf{elim}_*(P_1, P_2))^{\mathsf{dnf}}\right]^{\mathsf{mt}}$. Since by hypothesis $\ell \in \{|h| \geq |U| - n, |h| < |U| - n \mid n \in \mathbb{N}\}$, by Proposition 11, this literal is necessarily introduced by $\mathsf{elim}_*(P_1, P_2)$ and, by inspection of $\mathsf{elim}_*(P_1, P_2)$, one of the following must hold:
  - $\ell = |h| \geq \min_{M_1} + \min_{M_2}$, where $\min_{M_1}$ and/or $\min_{M_2}$ is of the form $|U| - n$. By the induction hypothesis ϕ_i contains a formula $\psi_1 \twoheadrightarrow \psi_2$ at polarity 1, for some $i = 1, 2$, and the proof is completed.
  - $\ell = |h| < \max_{M_1} + \max_{M_2} - 1$, where $\max_{M_1}$ and/or $\max_{M_2}$ is of the form $|U| - n$. The proof is similar, with polarity -1.
  - $\ell = |h| \geq \#_a(M_i) + |Y|_{M_i} + \min_{M_j}$, where $\min_{M_j}$ is of the form $|U| - n$. The proof is similar.
- $\phi = \phi_1 \multimap \phi_2 = \neg(\phi_1 \twoheadrightarrow \neg\phi_2)$: there exist minterms $M_i \in \mu^{fin}(\phi_i)$, $N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}$, for $i = 1, 2$, $P_1 \in (N_1)^{\mathsf{A}(M_1 \cup M_2)}$ and $Q_1 \in (P_1)^{M^a_2 \cup M^p_2}$, such that $M \in \left[\left(\mathsf{elim}^{fin}_{-\!\circ}(Q_1, N_2)\right)^{\mathsf{dnf}}\right]^{\mathsf{mt}}$. By inspection of $\mathsf{elim}^{fin}_{-\!\circ}(Q_1, N_2)$, one of the following cases must occur:

- $\ell = |h| \geq \min_{M_2} - \max_{M_1} - 1$, where $\min_{M_2}$ is of the form $|U| - n_2$. By the induction hypothesis, ϕ_2 contains a formula $\psi_1 \twoheadrightarrow \psi_2$ at polarity 1, and this formula also occurs at polarity 1 in ϕ, thus the proof is completed. Note that if $\max_{M_1} = |U| - n_1$ then either $\min_{M_2} = |U| - n_2$ and $|h| \geq \min_{M_2} - \max_{M_1} - 1 = |h| \geq n_1 - n_2$, or $\min_{M_2} = n_2 \in \mathbb{N}$ and $|h| \geq \min_{M_2} - \max_{M_1} - 1 = |h| \geq -|U| + (n_1 + n_2) = \bigwedge_{1 \leq n < n_1 + n_2} |U| \approx n \rightarrow |h| \geq n_1 + n_2 - n$ by Definition 2, thus $|h| \geq \min_{M_2} - \max_{M_1} - 1$ contains no literal of the above form.
- $\ell = |h| < \max_{M_2} - \min_{M_1}$. The proof is similar.
- $\ell = |h| < |U| - \min_{M_1} - \#_n(Y, M_1) + 1$. In this case since $(\phi_1 \twoheadrightarrow \neg\phi_2)$ occurs at polarity -1 in ϕ, the proof is completed.

(3) Let $\ell \in M \cap \{\mathsf{alloc}(x), \neg\mathsf{alloc}(x) \mid x \in \mathsf{Var}\}$ be a literal occurring in some minterm $M \in \mu^{inf}(\phi)$. The proof is by induction on the structure of ϕ:

- the cases $\phi = \mathsf{emp}$, $\phi = x \hookrightarrow \mathbf{y}$ and $\phi = x \approx y$ are trivial, because $\ell \notin \mu^{inf}(\phi)$.
- the cases $\phi = \phi_1 \wedge \phi_2$ and $\phi = \neg\phi_1$ are similar to point (2) of the Lemma.
- $\phi = \phi_1 * \phi_2$: there exist minterms $M_i \in \mu^{inf}(\phi_i)$, $N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}$ and $P_i \in (N_i)^{N^p_{3-i}}$, such that $M \in [(\mathsf{elim}_*(P_1, P_2))^{\mathsf{dnf}}]^{\mathsf{mt}}$, for all $i = 1, 2$. By inspection of $\mathsf{elim}_*(P_1, P_2)$, one of the following cases must occur:
  - $\ell = \neg\mathsf{alloc}(x)$ with $x \in \mathsf{nv}(M_1) \cap \mathsf{nv}(M_2)$. Assuming that the definition of $\mathsf{elim}_*(P_1, P_2)$ is changed according to Remark 3, it must be the case that $\neg\mathsf{alloc}(x)$ occurs at a positive polarity in M_1 or M_2. Then, by the induction hypothesis ϕ_i contains a subformula $\psi_1 \twoheadrightarrow \psi_2$ at polarity -1 with $x \in \mathsf{var}(\psi_1) \cup \mathsf{var}(\psi_2)$. But then $\psi_1 \twoheadrightarrow \psi_2$ also occurs at polarity -1 in ϕ and the proof is completed.
  - $\ell = \neg\mathsf{alloc}(x)$ with $x \in Y \subseteq \mathsf{nv}(M_j)$. Similar to the previous case.
- $\phi = \phi_1 \multimap \phi_2 = \neg(\phi_1 \twoheadrightarrow \neg\phi_2)$: there exist minterms $M_i \in \mu^{inf}(\phi_i)$, $N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}$, for $i = 1, 2$, $P_1 \in (N_1)^{\mathsf{A}(M_1 \cup M_2)}$ and $Q_1 \in (P_1)^{M^a_2 \cup M^p_2}$, such that $M \in \left[\left(\mathsf{elim}^{inf}_{\multimap}(Q_1, N_2)\right)^{\mathsf{dnf}}\right]^{\mathsf{mt}}$. By inspection of $\mathsf{elim}^{inf}_{\multimap}(Q_1, N_2)$, the only case possible is $\ell = \neg\mathsf{alloc}(x)$ (12) with $x \in \mathsf{av}(M_1)$, thus $x \in \mathsf{var}(\phi_1) \cup \mathsf{var}(\phi_2)$ and $(\phi_1 \twoheadrightarrow \neg\phi_2)$ occurs at polarity -1 in ϕ, which completes the proof.

(4) The proof is similar to point (3). The only difference is that $\mathsf{alloc}(x)$ may occur in the λ^{fin} subformula (14) of the $\mathsf{elim}^{fin}_{\multimap}(Q_1, N_2)$, in which case its polarity may be different from that of $\phi_1 \twoheadrightarrow \phi_2$. □

4.3 A Decision Problem

Given a quantifier-free SL^k formula ϕ, the number of minterms occurring in $\mu^{fin}(\phi)$ $[\mu^{inf}(\phi)]$ is exponential in the size of ϕ, in the worst case. Therefore, an optimal decision procedure cannot generate and store these sets explicitly, but rather must enumerate minterms lazily. We show that (i) the size of the minterms in $\mu^{fin}(\phi) \cup \mu^{inf}(\phi)$ is bounded by a polynomial in the size of ϕ (Corollary 1), and that (ii) the problem "*given a minterm M, does $M \in \mu^{fin}(\phi)$ [$\mu^{inf}(\phi)$] ?*" is in PSPACE (Lemma 8).

To start with, we define a measure on a quantifier-free formula ϕ, which bounds the size of the minterms in the sets $\mu^{fin}(\phi)$ and $\mu^{inf}(\phi)$, inductively on the structure of the formulae, as follows:

$$\mathcal{M}(x \approx y) \stackrel{\text{def}}{=} 0 \qquad \mathcal{M}(\bot) \stackrel{\text{def}}{=} 0$$
$$\mathcal{M}(\mathsf{emp}) \stackrel{\text{def}}{=} 1 \qquad \mathcal{M}(x \mapsto \mathbf{y}) \stackrel{\text{def}}{=} 2$$
$$\mathcal{M}(\neg\phi_1) \stackrel{\text{def}}{=} \mathcal{M}(\phi_1) \quad \mathcal{M}(\phi_1 \wedge \phi_2) \stackrel{\text{def}}{=} \max(\mathcal{M}(\phi_1), \mathcal{M}(\phi_2))$$

$$\mathcal{M}(\phi_1 * \phi_2) \stackrel{\text{def}}{=} \textstyle\sum_{i=1}^{2}(\mathcal{M}(\phi_i) + ||\mathsf{var}(\phi_i)||)$$
$$\mathcal{M}(\phi_1 \mathrel{-\!\!*} \phi_2) \stackrel{\text{def}}{=} \textstyle\sum_{i=1}^{2}(\mathcal{M}(\phi_i) + ||\mathsf{var}(\phi_i)||)$$

Proposition 13. *For any $n \in \mathbb{N}$, we have:*

$$\mathcal{M}(|h| \geq n) = \mathcal{M}(|U| \geq n) = n$$
$$\mathcal{M}(|h| \geq |U| - n) = n + 1$$

Proof: By induction on $n \geq 0$. □

Proposition 14. *For any formula ϕ, $\mathcal{M}(\phi) = O(\mathsf{size}(\phi)^2)$.*

Proof: By induction on ϕ. The most interesting cases are $\phi_1 * \phi_2$ and $\phi_1 \mathrel{-\!\!*} \phi_2$:

$$\begin{aligned}\mathcal{M}(\phi_1 * \phi_2) &= \textstyle\sum_{i=1}^{2}(\mathcal{M}(\phi_i) + ||\mathsf{var}(\phi_i)||) \\ &\leq \textstyle\sum_{i=1}^{2}(\mathcal{M}(\phi_i) + \mathsf{size}(\phi_i)) \\ &= O(\textstyle\sum_{i=1}^{2}(\mathsf{size}(\phi_i)^2 + \mathsf{size}(\phi_i)) \\ &= O((\mathsf{size}(\phi_1) + \mathsf{size}(\phi_2))^2)\end{aligned}$$

The case $\phi_1 \mathrel{-\!\!*} \phi_2$ is identical. □

Definition 7. *A minterm M is $\mathcal{M}$*-bounded *by a formula ϕ, if for each literal $\ell \in M$, the following hold: (i) $\mathcal{M}(\ell) \leq \mathcal{M}(\phi)$ if $\ell \in \{|h| \geq \min_{M_i}, |h| < \max_{M_i}\}$, and (ii) $\mathcal{M}(\ell) \leq 2\mathcal{M}(\phi) + 1$, if $\ell \in \{|U| \geq n, |U| < n \mid n \in \mathbb{N}\}$.*

Proposition 15. *Given minterms $M_1, \ldots, M_n$ all $\mathcal{M}$-bounded by ϕ, each minterm $M \in [M_1, \ldots, M_n]$ is also $\mathcal{M}$-bounded by ϕ.*

Proof: An immediate corollary of Proposition 11. □

Lemma 7. *Given a quantifier-free SL^k formula ϕ, each minterm $M \in \mu^{fin}(\phi) \cup \mu^{inf}(\phi)$ is $\mathcal{M}$-bounded by ϕ.*

Proof: We prove that each $M \in \mu^{fin}(\phi)$ is $\mathcal{M}$-bounded by ϕ. The proof for $M \in \mu^{inf}(\phi)$ follows from the observation that, because of the definition of $\mathsf{elim}^{inf}_{-\circ}$, for each $M \in \mu^{inf}(\phi)$ there exists $M' \in \mu^{fin}(\phi)$ such that $\mathcal{M}(M) \leq \mathcal{M}(M')$. By induction on the structure of ϕ:

- If $\phi = \mathsf{emp}$ then $\mu^{fin}(\phi) = \{|h| \geq 0 \wedge |h| < 1\}$, $\mathcal{M}(|h| \geq 0) = 0$, $\mathcal{M}(|h| < 1) = \mathcal{M}(|h| \geq 1) = 1$ and $\mathcal{M}(\mathsf{emp}) = 1$, by definition.
- If $\phi = x \mapsto \mathbf{y}$ then $\mu^{fin}(\phi) = \{x \hookrightarrow \mathbf{y} \wedge |h| \geq 1 \wedge |h| < 2\}$, $\mathcal{M}(|h| \geq 1) = 1$, $\mathcal{M}(|h| < 2) = 2$ and $\mathcal{M}(x \mapsto \mathbf{y}) = 2$, by definition.
- If $\phi = x \approx y$ then $\mu^{fin}(\phi) = \{x \approx y \wedge |h| \geq 0 \wedge |h| < \infty\}$ and $\mathcal{M}(|h| \geq 0) = \mathcal{M}(|h| < \infty) = 0$, by definition.
- If $\phi = \phi_1 \wedge \phi_2$, let $\ell \in M$ be a literal, where $M \in \mu^{fin}(\phi_1 \wedge \phi_2)$ is a minterm. Then $M \in [M_1, M_2]$, for some minterms $M_i \in \mu^{fin}(\phi_i)$, $i = 1, 2$ and the proof follows from Proposition 15, because M_i is $\mathcal{M}$-bounded by ϕ_i and $\mathcal{M}(\phi_i) \leq \mathcal{M}(\phi)$, thus M_i is $\mathcal{M}$-bounded by ϕ, for $i = 1, 2$.
- If $\phi = \neg\phi_1$ assume that $\mu^{fin}(\phi_1) = \{M_1, \ldots, M_m\}$. Let $\ell \in M$ be a literal, where $M \in \mu^{fin}(\neg\phi_1)$ is a minterm. Then $M \in \left[\left[\overline{\ell_1}\right]^{\mathsf{mt}}, \ldots, \left[\overline{\ell_n}\right]^{\mathsf{mt}}\right]$, for some literals $\ell_i \in M_i$, $i \in [1, m]$. By the induction hypothesis, $\overline{\ell_i}$ is $\mathcal{M}$-bounded by ϕ, for every $i \in 1, \ldots, n$, thus the same holds for ℓ_i. Since $\mathcal{M}(|h| \geq 0) = \mathcal{M}(|h| < \infty) = 0$, we deduce that $\left[\overline{\ell_i}\right]^{\mathsf{mt}}$ is $\mathcal{M}$-bounded by ϕ, and the proof follows from Proposition 15.
- If $\phi = \phi_1 * \phi_2$, let $\ell \in M$ be a literal, where $M \in \mu^{fin}(\phi_1 * \phi_2)$. Then there exist minterms $M_i \in \mu^{fin}(\phi_i)$, $N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}$ and $P_i \in (N_i)^{N^P_{3-i}}$, such that $M \in \left[(\mathsf{elim}_*(P_1, P_2))^{\mathsf{dnf}}\right]^{\mathsf{mt}}$, for $i = 1, 2$. First assume that ℓ is of the form $|h| \geq t$ or $|h| < t$. We only consider the case where ℓ occurs in $\mathsf{elim}_*(P_1, P_2)$, the rest of the cases follow from Proposition 15. We distinguish the following cases:
  - ℓ is a subformula of $|h| \geq \min_{P_1} + \min_{P_2} = |h| \geq \min_{M_1} + \min_{M_2}$, because $\min_{P_i} = \min_{M_i}$, for $i = 1, 2$, by Proposition 12. By the inductive hypothesis we have $\mathcal{M}(|h| \geq \min_{M_i}) \leq \mathcal{M}(\phi_i)$, for $i = 1, 2$. If $\min_{M_i} \in \mathbb{N}$ for $i = 1, 2$ then $\ell = |h| \geq \min_{M_1} + \min_{M_2}$ and we have:

    $$\begin{aligned}\mathcal{M}(\ell) = \mathcal{M}(|h| \geq \min_{M_1} + \min_{M_2}) &= \mathcal{M}(|h| \geq \min_{M_1}) + \mathcal{M}(|h| \geq \min_{M_2}) \\ &\leq \mathcal{M}(\phi_1) + \mathcal{M}(\phi_2) \leq \mathcal{M}(\phi).\end{aligned}$$

    If $\min_{M_i} = |U| - n_i$ and $n_i, \min_{M_{3-i}} \in \mathbb{N}$, then $\ell = |h| \geq \min_{M_1} + \min_{M_2}$ and we obtain:

    $$\begin{aligned}\mathcal{M}(\ell) = \mathcal{M}(|h| \geq \min_{M_1} + \min_{M_2}) &= \mathcal{M}(|h| \geq |U| - (n_i - \min_{M_{3-i}})) \\ &\leq \mathcal{M}(|h| \geq |U| - n_i) \\ &\leq \mathcal{M}(\phi_i) \leq \mathcal{M}(\phi).\end{aligned}$$

Otherwise, $\min_{M_i} = |U| - n_i$, for $i = 1, 2$, where $n_1, n_2 \in \mathbb{N}$, thus by Definition 2:

$$\begin{array}{ll} |h| \geq \min_{M_1} + \min_{M_2} & = \\ |h| \geq 2 \cdot |U| - n_1 - n_2 & = \\ |U| < 1 + n_1 + n_2 \wedge & \\ \bigwedge_{1 \leq n \leq n_1+n_2} |U| \approx n \rightarrow |h| \geq 2n - n_1 - n_2 & \end{array}$$

and either:

* $\ell \in \{|U| \geq n, |U| < n + 1\}$ for some $n \in [1, n_1 + n_2]$: we have $\mathcal{M}(\ell) \leq n + 1 \leq n_1 + n_2 + 1 \leq 2(\mathcal{M}(\phi_1) + \mathcal{M}(\phi_2)) + 1 = 2\mathcal{M}(\phi) + 1$, or
* $\ell = |h| \geq 2n - n_1 - n_2$ for some $n \in [1, n_1 + n_2]$: we have $\mathcal{M}(\ell) = 2n - n_1 - n_2 \leq n_1 + n_2 = \mathcal{M}(\phi_1) + \mathcal{M}(\phi_2) = \mathcal{M}(\phi)$.

- The proof in the case where ℓ is a subformula of $|h| < \max_{M_1} + \max_{M_2} - 1$ is analogous.
- $\ell = |h| \geq \#_a(P_i) + |Y|_{P_i} + \min_{P_{3-i}}$, where $Y \subseteq \mathsf{nv}(P_{3-i}) \setminus \mathsf{av}(P_i)$, for some $i = 1, 2$. Because $Y \cap \mathsf{av}(P_i) = \emptyset$, we have (Definition 3 and Proposition 12): $\#_a(P_i) + |Y|_{P_i} \leq \|\mathsf{var}(P_i)\| + \|\mathsf{var}(P_{3-i})\| \leq \|\mathsf{var}(\phi_1)\| + \|\mathsf{var}(\phi_2)\|$ and thus $\mathcal{M}(\ell) \leq \mathcal{M}(|h| \geq \min_{P_{3-i}}) + \|\mathsf{var}(\phi_1)\| + \|\mathsf{var}(\phi_2)\| \leq \mathcal{M}(\phi)$.

Now assume $\ell \in \{|U| \geq m, |U| < m \mid m \in \mathbb{N}\}$. Then one of the following holds:

- $\ell \in \mathsf{dc}(P_i)^u$, for some $i = 1, 2$, and we have two cases:
  * $\ell \in \{|U| \geq n_1 + n_2 + 1, |U| < n_1 + n_2\}$, where $\min_{P_i} = \min_{M_i} = n_1$ and $\max_{P_i} = \max_{M_i} = |U| - n_2$. By the induction hypothesis, we have $n_1, n_2 \leq \mathcal{M}(\phi_i)$, thus $\mathcal{M}(\ell) \leq 2\mathcal{M}(\phi_i) + 1 \leq 2\mathcal{M}(\phi) + 1$.
  * $\ell = |U| \geq \left\lceil \sqrt[k]{\max_{x \in \mathsf{av}(M)}(\delta_x(P_i) + 1)} \right\rceil$, in which case either $\mathsf{var}(M_1) \cup \mathsf{var}(M_2) = \emptyset$ so that $\left\lceil \sqrt[k]{\max_{x \in \mathsf{av}(M)}(\delta_x(P_i) + 1)} \right\rceil = 0$ and the proof is immediate, or we have $\mathcal{M}(\ell) \leq \sqrt[k]{\|\mathsf{var}(M_i)\|^k + 1} \leq |\mathsf{var}(M_i)| + 1 \leq 2\mathcal{M}(\phi) + 1$.
- $\ell = |U| > n_i + \#_a(P_i) + |Y|_{M_i}$, where $Y \subseteq \mathsf{nv}(M_{3-i}) \setminus \mathsf{av}(M_i)$ and $\max_{M_i} = |U| - n_i$, for some $i = 1, 2$. Because $Y \cap \mathsf{av}(P_i) = \emptyset$, we have $\#_a(P_i) + |Y|_{P_i} \leq \|\mathsf{var}(P_i)\| + \|\mathsf{var}(P_{3-i})\| \leq \|\mathsf{var}(\phi_1)\| + \|\mathsf{var}(\phi_2)\|$ and thus $\mathcal{M}(\ell) \leq \mathcal{M}(\phi_i) + \|\mathsf{var}(\phi_1)\| + \|\mathsf{var}(\phi_2)\| \leq 2\mathcal{M}(\phi) + 1$.

– If $\phi = \phi_1 \multimap \phi_2$, consider a literal $\ell \in M$, where $M \in \mu^{\mathit{fin}}(\phi_1 \multimap \phi_2)$. Then there exist minterms $M_i \in \mu^{\mathit{fin}}(\phi_i)$ and $N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}$, for $i = 1, 2$, and minterms $P_1 \in (N_1)^{\mathsf{A}(M_1 \cup M_2)}$ and $Q_1 \in (P_1)^{M_2^a \cup M_2^p}$, such that $M \in \left[\left(\mathsf{elim}^{\mathit{fin}}_{\multimap}(Q_1, N_2)\right)^{\mathsf{dnf}}\right]^{\mathsf{mt}}$. We only consider the case where ℓ occurs in $\mathsf{elim}^{\mathit{fin}}_{\multimap}(Q_1, N_2)$, in the remaining cases, the result follows directly from Proposition 15. If ℓ is of the form $|h| \geq t$ or $|h| < t$ then either:

- ℓ is a subformula of $|h| \geq \min_{N_2} - \max_{Q_1} - 1 = |h| \geq \min_{M_2} - \max_{M_1} - 1$, because $\min_{N_2} = \min_{M_2}$ and $\max_{Q_1} = \max_{P_1} = \max_{N_1} = \max_{M_1}$ by Proposition 12. Then $\min_{M_2} \in \{n_2, |U| - n_2\}$ and $\max_{M_1} \in \{n_1, |U| - n_1\}$ with $n_1, n_2 \in \mathbb{N}_\infty$, and by the induction hypothesis $n_i \leq \mathcal{M}(\phi_i)$. If $\max_{M_1} = n_1$ or $\min_{M_2} \neq n_2$, then by an inspection of the different cases and using Proposition 13, we have $\ell = |h| \geq \min_{M_2} - \max_{M_1} + 1$, thus:

  $$\mathcal{M}(\ell) = \mathcal{M}(|h| \geq \min_{M_2} - \max_{M_1} + 1) \leq n_1 + n_2 \leq \mathcal{M}(\phi_1) + \mathcal{M}(\phi_2) \leq \mathcal{M}(\phi)$$

  Otherwise, $\min_{M_2} = n_2$ and $\max_{M_1} = |U| - n_1$ hence either:
  - $\ell \in \{|U| \geq n, |U| < n + 1\}$, for some $n \in [1, n_1 + n_2 - 1]$ and we have $\mathcal{M}(\ell) \leq n + 1 \leq n_1 + n_2 \leq 2(\mathcal{M}(\phi_1) + \mathcal{M}(\phi_2)) + 1 = \mathcal{M}(\phi)$, or
  - $\ell = |h| \geq n_1 + n_2 - n$, for some $n \in [1, n_1 + n_2 - 1]$ and we have $\mathcal{M}(\ell) = n_1 + n_2 - n \leq n_1 + n_2 - 1 \leq \mathcal{M}(\phi_1) + \mathcal{M}(\phi_2) = \mathcal{M}(\phi)$.
- The case $\ell = |h| < \max_{N_2} - \min_{Q_1}$ is proved in a similar way.
- $\ell = |h| < |U| - \min_{Q_1} - \#_n(Y, Q_1) + 1$, for some $Y \subseteq \mathsf{var}(Q_1 \cup N_2)$. Because $\mathsf{nv}(Q_1) \subseteq \mathsf{nv}(P_1) \subseteq \mathsf{var}(\phi_1) \cup \mathsf{var}(\phi_2)$, we have $\#_n(Y, Q_1) \leq \|\mathsf{var}(\phi_1)\| + \|\mathsf{var}(\phi_2)\|$. Moreover, $\min_{Q_1} = \min_{M_1}$ by Proposition 12. We distinguish the following cases:
  - If $\min_{M_1} \in \mathbb{N}$, we compute:

    $$\begin{aligned} \mathcal{M}(\ell) &= \min_{M_1} + \#_n(Y, Q_1) - 1, \text{ by Proposition 13} \\ &\leq \mathcal{M}(\phi_1) + \|\mathsf{var}(\phi_1)\| + \|\mathsf{var}(\phi_2)\| \leq \mathcal{M}(\phi), \end{aligned}$$

    since $\mathcal{M}(|h| \geq \min_{M_1}) \leq \mathcal{M}(\phi_1)$, by the inductive hypothesis.
  - Otherwise, $\min_{M_1} = |U| - n_1$, for some $n_1 \in \mathbb{N}$, thus $\ell = |h| < n_1 - \#_n(Y, Q_1) + 1$. By Proposition 13, we have $\mathcal{M}(|h| \geq \min_{M_1}) = n_1 + 1$ and $\mathcal{M}(\ell) = n_1 - \#_n(Y, Q_1) + 1$, therefore:

    $$\begin{aligned} \mathcal{M}(\ell) &= \mathcal{M}(|h| \geq \min_{M_1}) - \#_n(Y, Q_1) \\ &\leq \mathcal{M}(\phi_1) \leq \mathcal{M}(\phi) \end{aligned}$$

If ℓ is of the form $|U| \geq m$ or $|U| < m$, with $m \in \mathbb{N}$, then either:
- if $\ell \in \mathsf{dc}(Q_1) \cup \mathsf{dc}(N_2)$ the argument is similar to the previous case $\phi = \phi_1 * \phi_2$,
- otherwise, $\ell = |U| \geq \min_{M_2} + \#_n(Y, M_1)$ and either $\min_{M_2} \in \mathbb{N}$, in which case $\mathcal{M}(\ell) = \min_{N_2} + \#_n(Y, Q_1) \leq \mathcal{M}(\phi_2) + \|\mathsf{var}(\phi_1)\| + \|\mathsf{var}(\phi_2)\| \leq \mathcal{M}(\phi)$ as in the previous, or $\min_{M_2} = |U| - n_2$, for some $n_2 \in \mathbb{N}$, in which case $\ell \equiv n_2 \geq \#_n(Y, Q_1)$ and $\mathcal{M}(\ell) = 0$. □

Corollary 1. *Given a quantifier-free* SL^k *formula* ϕ *and a minterm* $M \in \mu^{fin}(\phi) \cup \mu^{inf}(\phi)$, *we have* $\mathsf{size}(M) = \mathcal{O}(\mathsf{size}(\phi)^2)$.

Proof: We give the proof for $M \in \mu^{fin}(\phi)$, the case $M \in \mu^{inf}(\phi)$ being similar. Let $\ell \in M$ be a literal. We distinguish the following cases, based on the form of ℓ:

- $\ell \in \{\mathsf{alloc}(x), \neg\mathsf{alloc}(x) \mid x \in \mathsf{Var}\}$: ℓ occurs in ϕ or has been introduced by $\mu^{fin}(.)$, in which case, at most $2\|\mathsf{var}(\phi)\|$ such literals are introduced.
- $\ell \in \{x \hookrightarrow \mathbf{y}, \neg x \hookrightarrow \mathbf{y} \mid x \in \mathsf{Var}, \mathbf{y} \in \mathsf{Var}^k\}$: ℓ occurs in ϕ, since $\mu^{fin}(.)$ does not introduce literals of this form.
- $\ell \in \{x \approx y, \neg x \approx y \mid x, y \in \mathsf{Var}\}$: ℓ occurs in ϕ or has been introduced by $\mu^{fin}(.)$, in which case at most $2\|\mathsf{var}(\phi)\|^2$ such literals are introduced.
- $\ell \in \{|U| \geq n, |U| < n \mid n \in \mathbb{N}\}$: by Lemma 7, $\mathcal{M}(\ell) \leq 2\mathcal{M}(\phi) + 1$, thus $\mathsf{size}(\ell) = O(\mathsf{size}(\phi)^2)$ for each such literal. Furthermore, M contains at most two literals of this form (up to redundancy).
- $\ell \in \{|h| \geq \min_M, |h| < \max_M\}$: by Lemma 7, $\mathcal{M}(\ell) \leq \mathcal{M}(\phi)$ and consequently, $\mathsf{size}(\ell) = O(\mathsf{size}(\phi)^2)$ for each such literal. Furthermore, M contains exactly two literals of this form by definition of minterms.

Summing up, we obtain that $\mathsf{size}(M) = O(\mathsf{size}(\phi)^2)$. □

Proposition 16. *Let L be a set of literals and ϕ be a boolean combination of literals. The problem whether $L \in (\phi)^{\mathsf{dnf}}$ is in* $\mathsf{NSPACE}(\mathsf{size}(L) + \mathsf{size}(\phi))$.

Proof: W.l.o.g., we may assume that ϕ is in negation normal form. The algorithm is nondeterministic and proceeds recursively on the structure of ϕ:

- $\phi = \ell$ is a literal: then $(\phi)^{\mathsf{dnf}} = \{\ell\}$ hence it suffices to check that $L = \{\ell\}$, using $O(\mathsf{size}(L) + \mathsf{size}(\phi))$ space.
- $\phi = \phi_1 \vee \phi_2$: then $(\phi)^{\mathsf{dnf}} = (\phi_1)^{\mathsf{dnf}} \cup (\phi_2)^{\mathsf{dnf}}$ and we check that one of $L \in (\phi_1)^{\mathsf{dnf}}$ and $L \in (\phi_2)^{\mathsf{dnf}}$ holds. By the induction hypothesis, checking $L \in (\phi_i)^{\mathsf{dnf}}$ can be done using $O(\mathsf{size}(L) + \mathsf{size}(\phi_i))$ space. Since the working space used for $L \in (\phi_1)^{\mathsf{dnf}}$ can be reused for $L \in (\phi_2)^{\mathsf{dnf}}$, the entire check takes $O(\mathsf{size}(L) + \mathsf{size}(\phi))$ space.
- $\phi = \phi_1 \wedge \phi_2$: then $L \in (\phi)^{\mathsf{dnf}} \Leftrightarrow L = L_1 \cup L_2$, with $L_1 \in (\phi_1)^{\mathsf{dnf}}$ and $L_2 \in (\phi_2)^{\mathsf{dnf}}$, thus we guess two subsets L_1 and L_2 with $L_1 \cup L_2 = M$ and check that $L_i \in (\phi_i)^{\mathsf{dnf}}$, using $O(\mathsf{size}(L_i) + \mathsf{size}(\phi_i))$ space, for $i = 1, 2$. Since we must store L_2 during the check $L_1 \in (\phi_1)^{\mathsf{dnf}}$ and the working space can be reused for $L_2 \in (\phi_2)^{\mathsf{dnf}}$, the entire check takes $O(\mathsf{size}(L) + \mathsf{size}(\phi))$ space. □

Proposition 17. *Let L be a set of literals and let M_1, M_2 be minterms. Checking whether $L \in ((\mathsf{elim}_*(M_1, M_2))^{\mathsf{dnf}}$ is in* $\mathsf{NSPACE}(\mathsf{size}(L) + \mathsf{size}(M_1) + \mathsf{size}(M_2))$.

Proof: The algorithm proceeds by induction on the structure of $(\mathsf{elim}_*(M_1, M_2))^{\mathsf{dnf}}$ as in the proof of Proposition 16. The only difference concerns the subformulae η_{ij} (5) which cannot be constructed explicitly since they are of exponential size. However, η_{ij} is of positive polarity, and to check that $L \in \left(\eta_{ij}\right)^{\mathsf{dnf}}$, it suffices to guess a set of variables $Y \subseteq \mathsf{nv}(M_j) \setminus \mathsf{av}(M_i)$ and check whether:

$$L \in \left(\mathsf{alloc}(Y) \to (|h| \geq \#_a(M_i) + |Y|_{M_i} + \min_{M_j} \ \wedge \ \#_a(M_i) + |Y|_{M_i} < \max_{M_i})\right)^{\mathsf{dnf}}$$

The size of the above formula is of the order of $O(\mathsf{size}(M_1)+\mathsf{size}(M_2))$, thus $L \in ((\mathsf{elim}_*(M_1, M_2))^{\mathsf{dnf}}$ can be checked in $\mathsf{NSPACE}(\mathsf{size}(L) + \mathsf{size}(M_1) + \mathsf{size}(M_2))$, by Proposition 16. □

Proposition 18. *Let L be a set of literals and let M_1, M_2 be minterms. The problems whether $L \in \left((\mathsf{elim}^{fin}_{-\circ}(M_1, M_2)\right)^{\mathsf{dnf}}$ and $L \in \left((\mathsf{elim}^{inf}_{-\circ}(M_1, M_2)\right)^{\mathsf{dnf}}$ are both in* $\mathsf{NSPACE}(\mathsf{size}(L) + \mathsf{size}(M_1) + \mathsf{size}(M_2))$.

Proof: The proof is similar to that of Proposition 17 (again, the formula $\lambda^\dagger$ is exponential, but we do not have to construct it explicitly). □

Proposition 19. *Checking whether $M \in [M_1, \dots, M_n]$, where $M, M_1, \dots, M_n$ are minterms, $n \geq 2$, is in* $\mathsf{NSPACE}(\mathsf{size}(M) + (\mathsf{size}(M_1) + \ldots + \mathsf{size}(M_n))^2)$.

Proof: The proof is by induction on $n \geq 2$. If $n = 2$ then by definition of $[M_1, M_2]$ it suffices to check that $M = M_1^f \wedge M_1^e \wedge M_1^a \wedge M_1^p \wedge M_1^u \wedge M_2^f \wedge M_2^e \wedge M_2^a \wedge M_2^p \wedge M_2^u \wedge \mu \wedge \nu$ for some $\mu \in \mathrm{minh}(M_1, M_2)$, $\nu \in \mathrm{maxh}(M_1, M_2)$. By definition, the size of each formula in $\mathrm{minh}(M_1, M_2) \cup \mathrm{maxh}(M_1, M_2)$ is of the order of $O(\mathsf{size}(M_1) + \mathsf{size}(M_2))$, thus the algorithm requires $O(\mathsf{size}(M) + \mathsf{size}(M_1) + \mathsf{size}(M_2))$ space.

If $n > 2$, $M \in [M_1, \dots, M_n] \Leftrightarrow M \in [M', M_n]$ for some $M' \in [M_1, \dots, M_{n-1}]$. By Proposition 11, the literals in M' are either literals from $M_1, \dots, M_{n-1}$ or occur in $\{|U| \geq m_1 + m_2, |U| < m_1 + m_2, |U| \geq m_1 + m_2 + 1, |U| < m_1 + m_2 + 1\}$, where $M_1 \cup \cdots \cup M_{n-1}$ contains two literals ℓ_1 and ℓ_2 and ℓ_i is of the form $|h| \geq m_i, |h| < m_i, |h| \geq |U| - m_i$ or $|h| < |U| - m_i$, for $i = 1, 2$. Thus $\mathsf{size}(M') \leq \sum_{i=1}^{n-1} \mathsf{size}(M_i)$. The nondeterministic algorithm guesses and stores a minterm M_1' of size at most $\sum_{i=1}^{n-1} \mathsf{size}(M_i)$ and checks that $M \in \left[M_1', M_n\right]$ and that $M_1' \in [M_1, \dots, M_{n-1}]$. According to the base case $n = 2$, the first check takes up $O(\mathsf{size}(M)+\mathsf{size}(M_1')+\mathsf{size}(M_n)) = O(\mathsf{size}(M) + \sum_{i=1}^{n} \mathsf{size}(M_i))$ space, and the second check takes space $O(\mathsf{size}(M_1') + (\sum_{i=1}^{n-1} \mathsf{size}(M_i))^2) = O((\sum_{i=1}^{n} \mathsf{size}(M_i))^2)$, by the induction hypothesis. Because we only need to store M_1' between the two checks, the algorithm takes $O(\mathsf{size}(M) + (\sum_{i=1}^{n} \mathsf{size}(M_i))^2)$ space. □

Proposition 20. *Let M be a minterm and let L be a set of literals. The problem of checking whether $M = [L]^{\mathsf{mt}}$ is in* $\mathsf{NSPACE}(\mathsf{size}(M) + (\sum_{\ell \in L} \mathsf{size}(\ell))^2)$.

Proof: By definition, $[L]^{\mathsf{mt}} = [[\ell_1]^{\mathsf{mt}}, \dots, [\ell_n]^{\mathsf{mt}}]$, with $L = \{\ell_1, \dots, \ell_n\}$, and each minterm $[\ell_i]^{\mathsf{mt}}$ is of size $O(\mathsf{size}(\ell_i))$, thus the proof follows immediately from Proposition 19. □

Lemma 8. *Given a minterm M and an SL^k formula ϕ, the problems of checking whether $M \in \mu^{fin}(\phi)$ and $M \in \mu^{inf}(\phi)$ are in PSPACE.*

Proof: We show the existence of a nondeterministic algorithm that decides $M \in \mu^{fin}(\phi)$ in space $O(\mathsf{size}(M) + \mathsf{size}(\phi)^8)$. The PSPACE upper bound is by an application of Savitch's Theorem [15]. We only give the proof for $M \in \mu^{fin}(\phi)$, the proof for $M \in \mu^{inf}(\phi)$ being similar and omitted. By induction on the structure of ϕ, we distinguish the following cases:

- $\phi = \mathsf{emp}$: we check $M = |h| \approx 0$ in space $O(\mathsf{size}(M) + \mathsf{size}(\phi))$.
- $\phi = x \mapsto \mathbf{y}$: we check $M = \{x \hookrightarrow \mathbf{y} \wedge |h| \approx 1\}$ in space $O(\mathsf{size}(M) + \mathsf{size}(\phi))$.
- $\phi = \phi_1 \wedge \phi_2$: $M \in \mu^{fin}(\phi) \Leftrightarrow M \in [M_1, M_2]$ with $M_i \in \mu^{fin}(\phi_i)$, for every $i = 1, 2$. Since, by Corollary 1, $\mathsf{size}(M_i) = O(\mathsf{size}(\phi_i)^2) = O(\mathsf{size}(\phi)^2)$, for $i = 1, 2$, it suffices to guess two such minterms M_1 and M_2, check that $M_i \in \mu^{fin}(\phi_i)$, $i = 1, 2$ and that $M \in [M_1, M_2]$. By the induction hypothesis, checking $M_i \in \mu^{fin}(\phi_i)$ requires space $O(\mathsf{size}(M_i) + \mathsf{size}(\phi_i)^8)$, for each $i = 1, 2$, and by the proof of Proposition 19 in the case $n = 2$, checking $M \in [M_1, M_2]$ requires space $O(\mathsf{size}(M) + \mathsf{size}(M_1) + \mathsf{size}(M_2)) = O(\mathsf{size}(M) + \mathsf{size}(\phi))$. Since we only need to store M_1 and M_2 between the checks, the entire procedure takes space $O(\mathsf{size}(M) + \mathsf{size}(\phi)^8)$.
- $\phi = \neg\phi_1$: $M \in \mu^{fin}(\phi)$ if and only if $M \in \left[\left[\overline{\ell_1}\right]^{\mathsf{mt}}, \ldots, \left[\overline{\ell_m}\right]^{\mathsf{mt}}\right]$, for some literals $\ell_i \in M_i$, $i \in [1, m]$, where $\mu^{fin}(\phi) = \{M_1, \ldots, M_m\}$. For any $i \in [1, m]$, we distinguish the following cases:
  - if $\ell_i \in \left\{x \hookrightarrow \mathbf{y}, \neg x \hookrightarrow \mathbf{y} \mid x \in \mathsf{Var}, \mathbf{y} \in \mathsf{Var}^k\right\}$ then ℓ_i occurs in ϕ_1, thus there are at most $\mathsf{size}(\phi_1)$ such literals,
  - if $\ell_i \in \{x \approx y, \neg x \approx y \mid x, y \in \mathsf{Var}\}$ then there are at most $2\|\mathsf{var}(\phi)\|^2$ such literals,
  - if $\ell_i \in \{|U| \geq n, |U| < n \mid n \in \mathbb{N}\}$, by Lemma 7, $\mathcal{M}(\ell_i) \leq 2\mathcal{M}(\phi_1) + 1$, thus there are at most $2\mathcal{M}(\phi_1) + 1 = O(\mathsf{size}(\phi_1))^2$ such literals.

  Summing up, we obtain that $\|\{\ell_i \mid i \in [1, m]\}\| = O(\mathsf{size}(\phi_1)^2)$. Thus it suffices to guess a set $\left\{\ell'_1, \ldots, \ell'_n\right\}$ of literals and a set of minterms $\left\{M'_1, \ldots, M'_n\right\}$ such that $\ell'_i \in M'_i$, where $n = O(\mathsf{size}(\phi_1)^2)$ and $\mathsf{size}(M'_i) = O(\mathsf{size}(\phi_1)^2)$, for all $i \in [1, n]$. Then we can check that:
  - $M'_i \in \mu^{fin}(\phi_1)$, which can be done in space $O(\mathsf{size}(M'_i) + \mathsf{size}(\phi_1)^8) = O(\mathsf{size}(\phi_1)^2 + \mathsf{size}(\phi_1)^8) = O(\mathsf{size}(\phi_1)^8)$, by the inductive hypothesis,
  - $M \in \left[\left[\overline{\ell_1}\right]^{\mathsf{mt}}, \ldots, \left[\overline{\ell_n}\right]^{\mathsf{mt}}\right]$, which can be done in space $O(\mathsf{size}(M) + (n \cdot \mathsf{size}(\phi_1)^2)^2) = O(\mathsf{size}(M) + \mathsf{size}(\phi_1)^8)$, by Proposition 19.

  To ensure that the set $\{\ell_1, \ldots, \ell_m\}$ contains no literal other than $\ell'_1, \ldots, \ell'_n$, we also have to check that every minterm M_j, for $j \in [1, m]$ contains a literal ℓ'_i, for some $i \in [1, n]$. To this aim, we use a non deterministic algorithm for the complement: we guess a minterm M' $\mathcal{M}$-bounded by ϕ_1, check that

$M' \in \mu(\phi_1)$ and that it contains no literal ℓ_i, for $i \in [1,n]$. By the inductive hypothesis, this is possible in space $\mathcal{O}(\mathsf{size}(M')+\mathsf{size}(\phi_1)^8) = \mathcal{O}(\mathsf{size}(\phi_1)^2 + \mathsf{size}(\phi_1)^8) = \mathcal{O}(\phi_1^8)$. Then, checking that every minterm M_j, for $j \in [1,m]$ contains a literal ℓ'_i, for some $i \in [1,n]$ can be done in the same amount of space, using a nondeterministic algorithm, see e.g. [1, Corollary 4.21].

- $\phi = \phi_1 * \phi_2$: $M \in \mu^{fin}(\phi)$ iff there exist minterms $M_i \in \mu(\phi_i)$, $N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}$ and $P_i \in (N_i)^{N^p_{3-i}}$, such that $M \in [(\mathsf{elim}_*(P_1,P_2))^{\mathsf{dnf}}]^{\mathsf{mt}}$, for $i = 1,2$. We first guess minterms M_1, M_2 of size $\mathcal{O}(\mathsf{size}(\phi_1)^2)$ and $\mathcal{O}(\mathsf{size}(\phi_2)^2)$, respectively, check that $M_i \in \mu^{fin}(\phi_i)$, then guess $N_i \in (M_i)^{\mathsf{E}(M_1 \cup M_2)}$ and $P_i \in (N_i)^{N^p_{3-i}}$, for $i = 1,2$. This is feasible since by definition each minterm in these sets is of size $\mathcal{O}(\mathsf{size}(M_1) + \mathsf{size}(M_2))$. Next, we guess minterms M', M'', of size $\mathcal{O}(\mathsf{size}(M_1) + \mathsf{size}(M_2))$ as well, and check that $M' \in (\mathsf{elim}_*(P_1,P_2))^{\mathsf{dnf}}$ in space $\mathcal{O}(\mathsf{size}(M')+\mathsf{size}(P_1)+\mathsf{size}(P_2))$, by Proposition 19 and $M'' \in [M']^{\mathsf{mt}}$ in space $\mathcal{O}(\mathsf{size}(M'') + \mathsf{size}(M')^2)$, by Proposition 20.
- $\phi_1 \multimap \phi_2$: the proof is similar to the previous case. □

Corollary 2. *Given a finite* FO *structure* $\mathcal{S} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$ *and a formula* $\forall y_1 \ldots \forall y_m \,.\, \phi$, *where* ϕ *is quantifier-free, the problem* $\mathcal{S} \models \tau(\forall y_1 \ldots \forall y_m \,.\, \bigvee_{M \in \mu^\dagger(\phi)} M)$ *is in* PSPACE*, for each* $\dagger \in \{fin, inf\}$.

Proof: We have the equivalences:

$$\begin{aligned}
&\neg\tau(\forall y_1 \ldots \forall y_m \,.\, \textstyle\bigvee_{M \in \mu^\dagger(\phi)} M) \equiv \\
&\neg\forall y_1 \ldots \forall y_m \,.\, \tau(\textstyle\bigvee_{M \in \mu^\dagger(\phi)} M) \equiv \\
&\exists y_1 \ldots \exists y_m \,.\, \neg\tau(\textstyle\bigvee_{M \in \mu^\dagger(\phi)} M) \equiv \\
&\exists y_1 \ldots \exists y_m \,.\, \tau(\neg \textstyle\bigvee_{M \in \mu^\dagger(\phi)} M) \overset{\text{(Lemma 5)}}{\equiv} \\
&\exists y_1 \ldots \exists y_m \,.\, \tau(\textstyle\bigvee_{M \in \mu^\dagger(\neg\phi)} M) \equiv \\
&\textstyle\bigvee_{M \in \mu^\dagger(\neg\phi)} \exists y_1 \ldots \exists y_m \,.\, \tau(M).
\end{aligned}$$

To check that $\mathcal{S} \not\models \tau(\forall y_1 \ldots \forall y_m \,.\, \bigvee_{M \in \mu^\dagger(\phi)} M)$, we guess locations $\ell_1, \ldots, \ell_m \in \mathfrak{U}$ and a minterm M that is $\mathcal{M}$-bounded by ϕ, then check that $M \in \mu^\dagger(\neg\phi)$ and that $(\mathfrak{U}, \mathfrak{s}[y_1 \leftarrow \ell_1] \ldots [y_m \leftarrow \ell_m], \mathfrak{i}) \models \tau(M)$. The first check is in PSPACE, by Lemma 8. The second check is also in PSPACE, because $\tau(M)$ is a BSR(FO) formula of size polynomially bounded by $\mathsf{size}(M)$, and the only quantifiers introduced by $\tau(\ell)$, where $\ell \in M$ is a literal are:

- $\exists y_1, \ldots \exists y_k \,.\, \mathfrak{p}(x, y_1, \ldots, y_k)$ if $\ell = \mathsf{alloc}(x)$, and
- $\forall y_1, \ldots \forall y_k \,.\, \neg\mathfrak{p}(x, y_1, \ldots, y_k)$ if $\ell = \neg\mathsf{alloc}(x)$.

In both cases, one can check whether $\mathcal{S} \models \ell$, by inspection of $\mathfrak{p}^{\mathfrak{i}}$, which requires no additional space. Finally, PSPACE is closed under complement (see, e.g., [1, Corollary 4.21]), which concludes the proof. □

5 Bernays-Schönfinkel-Ramsey SL^k

This section gives the main results of the paper, concerning the (un)decidability of the (in)finite satisfiability problems within the $\mathsf{BSR}(\mathsf{SL}^k)$ fragment. From the satisfiability point of view, we can assume w.l.o.g. that $\mathsf{BSR}(\mathsf{SL}^k)$ is the set of sentences $\forall y_1 \ldots \forall y_m \,.\, \phi$, where ϕ is a quantifier-free SL^k formula, with $\mathsf{var}(\phi) = \{x_1, \ldots, x_n,$
$y_1, \ldots, y_m\}$, where the existentially quantified variables $x_1, \ldots, x_n$ are left free.

First, we show that, contrary to $\mathsf{BSR}(\mathsf{FO})$, the satisfiability of $\mathsf{BSR}(\mathsf{SL}^k)$ is undecidable for $k \geq 2$. Second, we carve two nontrivial fragments of $\mathsf{BSR}(\mathsf{SL}^k)$, for which the infinite and finite satisfiability problems are both PSPACE-complete. Technically, these fragments are defined based on restrictions of (i) polarities of the occurrences of the separating implication, and (ii) occurrences of universally quantified variables in the scope of separating implications.

These results draw a rather precise chart of decidability within the $\mathsf{BSR}(\mathsf{SL}^k)$ fragment, the only remaining gap being the decidability for the case $k = 1$. Indeed, it is known that the fragment of SL^1 whose formulae do not contain the separating implication is decidable but not elementary recursive [3]. However, the decidability status for $\mathsf{BSR}(\mathsf{SL}^1)$ with unrestricted uses of the separating implication is still open.

5.1 Undecidability of $\mathsf{BSR}(\mathsf{SL}^k)$

We consider the finite satisfiability problem of the $[\forall, (0), (2)]_=$ fragment of FO, which consists of sentences of the form $\forall x \,.\, \phi(x)$, where ϕ is a quantifier-free boolean combination of atomic propositions $t_1 \approx t_2$, and t_1, t_2 are terms built using two function symbols f and g, of arity one, the variable x and constant c. It is known[9] that finite satisfiability is undecidable for $[\forall, (0), (2)]_=$

Given a sentence $\varphi = \forall x \,.\, \phi(x)$ in $[\forall, (0), (2)]_=$, we proceed by first *flattening* each term in ϕ consisting of nested applications of f and g. The result is an equivalent sentence $\varphi_{flat} = \forall x_1 \ldots \forall x_n \,.\, \phi_{flat}$, in which the only terms are x_i, c, $f(x_i)$, $g(x_i)$, $f(c)$ and $g(c)$, for $i \in [1, n]$. For example, the formula $\forall x \,.\, f(g(x)) \approx c$ is flattened into $\forall x_1 \forall x_2 \,.\, g(x_1) \not\approx x_2 \vee f(x_2) \approx c$. The formal construction is standard and thus omitted. We define the following $\mathsf{BSR}(\mathsf{SL}^2)$ sentences, for each $\dagger \in \{\mathit{fin}, \mathit{inf}\}$:

$$\begin{aligned} \varphi^{\dagger}_{\mathsf{sl}} \stackrel{\mathsf{def}}{=} & \ \alpha^{\dagger} \wedge x_c \hookrightarrow (y_c, z_c) \wedge \\ & \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n \forall z_1 \ldots \forall z_n \,.\, \bigwedge_{i=1}^{n} (x_i \hookrightarrow (y_i, z_i) \rightarrow \phi_{\mathsf{sl}}) \end{aligned} \tag{17}$$

[9] See e.g. [2, Theorem 4.1.8].

where[10]:

$$\alpha^{fin} \stackrel{\text{def}}{=} \forall x \,.\, \mathsf{alloc}(x) \text{ or } \alpha^{fin} \stackrel{\text{def}}{=} |h| \geq |U| - 0$$
$$\alpha^{inf} \stackrel{\text{def}}{=} \forall x \forall y \forall z \,.\, x \hookrightarrow (y,z) \rightarrow \mathsf{alloc}(y) \wedge \mathsf{alloc}(z)$$

and ϕ_{sl} is obtained from ϕ_{flat} by replacing each occurrence of c by x_c, each term $f(c)$ $[g(c)]$ by y_c $[z_c]$ and each term $f(x_i)$ $[g(x_i)]$ by y_i $[z_i]$. Next, we show that φ and φ_{sl} are equisatisfiable, which permits to deduce that:

Theorem 1. *The finite and infinite satisfiability problems are undecidable for* $\mathsf{BSR}(\mathsf{SL}^k)$.

Proof Let $\varphi = \forall x \,.\, \phi$ be a sentence from $[\forall, (0), (2)]_=$. We show that the following statements are equivalent:

1. φ has a finite model $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$,
2. $\varphi^{fin}_{\mathsf{sl}}$ has a finite model $(\mathfrak{U}, \mathfrak{s}', \mathfrak{h})$, and
3. $\varphi^{inf}_{\mathsf{sl}}$ has an infinite model $(\mathfrak{U}^\infty, \mathfrak{s}', \mathfrak{h})$.

"(1) ⇒ (2)" We define the store $\mathfrak{s}' \stackrel{\text{def}}{=} \mathfrak{s}[x_c \leftarrow c^{\mathfrak{i}}, y_c \leftarrow f^{\mathfrak{i}}(c^{\mathfrak{i}}), z_c \leftarrow g^{\mathfrak{i}}(c^{\mathfrak{i}})]$ and the heap $\mathfrak{h}$ such that $\mathrm{dom}(\mathfrak{h}) = \mathfrak{U}$ and $\mathfrak{h}(\ell) \stackrel{\text{def}}{=} (f^{\mathfrak{i}}(\ell), g^{\mathfrak{i}}(\ell))$, for all $\ell \in \mathfrak{U}$. By construction, we have $(\mathfrak{U}, \mathfrak{s}', \mathfrak{h}) \models \alpha^{fin} \wedge x_c \hookrightarrow (y_c, z_c)$, because $\mathrm{dom}(\mathfrak{h}) = \mathfrak{U}$ and $\mathfrak{h}(c^{\mathfrak{i}}) = (f^{\mathfrak{i}}(c^{\mathfrak{i}}), g^{\mathfrak{i}}(c^{\mathfrak{i}}))$. Consider a store $\mathfrak{s}'' \stackrel{\text{def}}{=} \mathfrak{s}'[x_i \leftarrow \ell_i, y_i \leftarrow \ell'_i, z_i \leftarrow \ell''_i \mid i = 1, \ldots, n]$, for an arbitrary set $\{\ell_i, \ell'_i, \ell''_i \mid i \in [1,n]\} \subseteq \mathfrak{U}$ and assume that $(\mathfrak{U}, \mathfrak{s}'', \mathfrak{h}) \models \bigwedge_{i=1}^n x_i \hookrightarrow (y_i, z_i)$. Then by definition of $\mathfrak{h}$, for all $i \in [1,n]$, we have $\ell'_i = f^{\mathfrak{i}}(\ell_i)$ and $\ell''_i = g^{\mathfrak{i}}(\ell_i)$; hence, $(\mathfrak{U}, \mathfrak{s}'', \mathfrak{h}) \models \phi_{\mathsf{sl}}$. Since ℓ_i, ℓ'_i and ℓ''_i are arbitrary, for $i \in [1,n]$, this proves that $(\mathfrak{U}, \mathfrak{s}', \mathfrak{h})$ is a finite model of $\varphi^{fin}_{\mathsf{sl}}$.

"(2) ⇒ (3)" We define $\mathfrak{U}^\infty \stackrel{\text{def}}{=} \mathfrak{U} \uplus L$, where L is an infinite set of locations not in $\mathfrak{U}$. Clearly $(\mathfrak{U}^\infty, \mathfrak{s}', \mathfrak{h}) \models \alpha^{inf}$, because $x \hookrightarrow (y,z)$ is false for any extension of $\mathfrak{s}'$ with a pair of the form $[x \leftarrow \ell]$, $[y \leftarrow \ell]$ or $[z \leftarrow \ell]$, where $\ell \in L$. Furthermore, the valuation of $x_c \hookrightarrow (y_c, z_c)$ is unchanged between $(\mathfrak{U}, \mathfrak{s}', \mathfrak{h})$ and $(\mathfrak{U}^\infty, \mathfrak{s}', \mathfrak{h})$. Consider a store $\mathfrak{s}'' \stackrel{\text{def}}{=} \mathfrak{s}'[x_i \leftarrow \ell_i, y_i \leftarrow \ell'_i, z_i \leftarrow \ell''_i \mid i = 1, \ldots, n]$, for an arbitrary set $\{\ell_i, \ell'_i, \ell''_i \mid i \in [1,n]\} \subseteq \mathfrak{U}$ and assume that $(\mathfrak{U}, \mathfrak{s}'', \mathfrak{h}) \models \bigwedge_{i=1}^n x_i \hookrightarrow (y_i, z_i)$. Then necessarily, $\left\{\ell_i, \ell'_i, \ell''_i \mid i \in [1,n]\right\} \cap L = \emptyset$. Next, we show that $(\mathfrak{U}, \mathfrak{s}'', \mathfrak{h}) \models \phi_{\mathsf{sl}} \Leftrightarrow (\mathfrak{U}^\infty, \mathfrak{s}'', \mathfrak{h}) \models \phi_{\mathsf{sl}}$, by induction on the structure of ϕ_{sl}. Since $(\mathfrak{U}, \mathfrak{s}'', \mathfrak{h}) \models \phi_{\mathsf{sl}}$ by the hypothesis, we have $(\mathfrak{U}^\infty, \mathfrak{s}'', \mathfrak{h}) \models \phi_{\mathsf{sl}}$, thus $(\mathfrak{U}^\infty, \mathfrak{s}, \mathfrak{h}) \models \varphi^{inf}_{\mathsf{sl}}$.

"(3) ⇒ (1)" Let $\mathfrak{U} \stackrel{\text{def}}{=} \mathrm{dom}(\mathfrak{h}) \cup \{\ell_1, \ell_2 \mid \exists \ell \in \mathfrak{U}^\infty \,.\, \mathfrak{h}(\ell) = (\ell_1, \ell_2)\}$. Since $\mathfrak{h}$ is finite, so is $\mathfrak{U}$. Let $\mathfrak{s}$ be an arbitrary[11] store on $\mathfrak{U}$ and define $\mathfrak{i}$ such that:

- $c^{\mathfrak{i}} = \mathfrak{s}'(x_c)$, and,
- for each $\ell \in \mathfrak{U}$, such that $\mathfrak{h}(\ell) = (\ell', \ell'')$, we have $f^{\mathfrak{i}}(\ell) = \ell'$ and $g^{\mathfrak{i}}(\ell) = \ell''$.

[10] Note that the two definitions of α^{fin} are equivalent.
[11] The store is arbitrary because φ contains no free variables.

Note that $c^{\mathfrak{i}} \in \mathfrak{U}$, because by hypothesis $(\mathfrak{U}^\infty, \mathfrak{s}', \mathfrak{h}) \models x_c \hookrightarrow (y_c, z_c)$, hence $\mathfrak{s}'(x_c) \in \mathrm{dom}(\mathfrak{h})$. Similarly, $f^{\mathfrak{i}}(\ell), g^{\mathfrak{i}}(\ell) \in \mathfrak{U}$, for each $\ell \in \mathfrak{U}$, by the definition of $\mathfrak{U}$. Moreover, since $(\mathfrak{U}^\infty, \mathfrak{s}', \mathfrak{h}) \models \alpha^{inf}$ we obtain that $f^{\mathfrak{i}}$ and $g^{\mathfrak{i}}$ are well-defined total functions. For each set $\{\ell_i \mid i = 1, \ldots, n\} \subseteq \mathfrak{U}$, the function $\mathfrak{s}'' = \mathfrak{s}[x_i \leftarrow \ell_i, y_i \leftarrow f^{\mathfrak{i}}(\ell_i), z_i \leftarrow g^{\mathfrak{i}}(\ell_i) \mid i = 1, \ldots, n]$ is a store on $\mathfrak{U}^\infty$ such that $(\mathfrak{U}^\infty, \mathfrak{s}'', \mathfrak{h}) \models x_i \hookrightarrow (y_i, z_i)$ for every $i \in [1, n]$, hence $(\mathfrak{U}^\infty, \mathfrak{s}'', \mathfrak{h}) \models \phi_{\mathsf{sl}}$. By induction on the structure of ϕ, one shows that $(\mathfrak{U}^\infty, \mathfrak{s}'', \mathfrak{h}) \models \phi_{\mathsf{sl}} \Leftrightarrow (\mathfrak{U}, \mathfrak{s}'', \mathfrak{i}) \models \phi_{flat}$. Since $(\mathfrak{U}^\infty, \mathfrak{s}'', \mathfrak{h}) \models \phi_{\mathsf{sl}}$, we have $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \phi_{flat}$. □

5.2 Two Decidable Fragments of $\mathsf{BSR}(\mathsf{SL}^k)$

The reductions (17) use either positive occurences of $\mathsf{alloc}(x)$, where x is universally quantified, or test formulae $|h| \geq |U| - n$. We obtain decidable subsets of $\mathsf{BSR}(\mathsf{SL}^k)$ by eliminating the positive occurrences of both (i) $\mathsf{alloc}(x)$, with x universally quantified, and (ii) $|h| \geq |U| - n$, from $\mu^\dagger(\phi)$, where $\dagger \in \{fin, inf\}$ and $\forall y_1 \ldots \forall y_m . \phi$ is any $\mathsf{BSR}(\mathsf{SL}^k)$ formula. Note that $\mu^{inf}(\phi)$ does not contain formulae of the form $|h| \geq |U| - n$ anyway, which explains why slightly less restrictive conditions are needed for infinite structures.

Definition 8. *Given an integer $k \geq 1$, we define:*

1. $\mathsf{BSR}^{inf}(\mathsf{SL}^k)$ *as the set of sentences $\forall y_1 \ldots \forall y_m . \phi$ such that for all $i \in [1, m]$ and all formulae $\psi_1 \twoheadrightarrow \psi_2$ occurring at polarity 1 in ϕ, we have $y_i \notin \mathsf{var}(\psi_1) \cup \mathsf{var}(\psi_2)$,*
2. $\mathsf{BSR}^{fin}(\mathsf{SL}^k)$ *as the set of sentences $\forall y_1 \ldots \forall y_m . \phi$ such that no formula $\psi_1 \twoheadrightarrow \psi_2$ occurs at polarity 1 in ϕ.*

Note that $\mathsf{BSR}^{fin}(\mathsf{SL}^k) \subsetneq \mathsf{BSR}^{inf}(\mathsf{SL}^k) \subsetneq \mathsf{BSR}(\mathsf{SL}^k)$, for any $k \geq 1$.

We start by showing decidability, in PSPACE, of the infinite satisfiability problem for the $\mathsf{BSR}^{inf}(\mathsf{SL}^k)$ fragment. To this end, given a $\mathsf{BSR}(\mathsf{FO})$ formula φ, whose only function of a strictly positive arity is the boolean function $\mathfrak{p}$, we provide an axiom φ_∞ that guarantees the existence of an infinite model for φ.

Definition 9. *Let $\varphi = \forall y_1 \ldots \forall y_m . \phi$ be a $\mathsf{BSR}(\mathsf{FO})$ formula, where $\{x_1, \ldots, x_n\}$ is the set of constants and free variables in φ and ϕ is quantifier-free. Let $c_1, \ldots, c_m$ be pairwise distinct constants such that $\{c_1, \ldots, c_m\} \cap \{x_1, \ldots, x_n\} = \emptyset$.*

We define:

$$\varphi_\infty \stackrel{\text{def}}{=} \bigwedge_{i=1}^{m} \forall z_1 \ldots \forall z_k \,.\, \neg \mathfrak{p}(c_i, z_1, \ldots, z_k) \;\wedge$$
$$\bigwedge_{\substack{i,j \in [1,m] \\ i \neq j}} c_i \not\approx c_j \;\wedge\; \bigwedge_{\substack{i \in [1,n] \\ j \in [1,m]}} x_i \not\approx c_j \;\wedge$$
$$\forall x \forall z_1 \ldots \forall z_k \,.\, \bigwedge_{\substack{\ell \in [1,k] \\ j \in [1,m]}} \neg \mathfrak{p}(x, z_1, \ldots, z_{\ell-1}\, c_j, z_{\ell+1}, \ldots, z_k)$$

Proposition 21. *Let $\varphi = \forall y_1 \ldots \forall y_m \,.\, \phi$ be a* BSR(FO) *formula, where ϕ is a quantifier-free formula built on a signature containing only constants and the boolean function symbol $\mathfrak{p}$, of arity $k+1$. The formula $\varphi \wedge \varphi_\infty$ is satisfiable iff φ has an infinite model $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$, such that $\|\mathfrak{p}^{\mathfrak{i}}\| \in \mathbb{N}$.*

Proof: Let $\mathcal{S} = (\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$ be a model of $\varphi \wedge \varphi_\infty$. Since $\varphi \wedge \varphi_\infty$ is in BSR(FO), we may assume that $\mathfrak{U}$ is finite by [2, Proposition 6.2.17], hence $\|\mathfrak{p}^{\mathfrak{i}}\| \in \mathbb{N}$ as well. Consider an extension $\mathfrak{U}'$ of $\mathfrak{U}$ obtained by adding infinitely many new elements. Let $\mathbf{a} = (a_1, \ldots, a_m)$ be a vector of elements in $\mathfrak{U}'$ and $\mathbf{b} = (b_1, \ldots, b_m)$ be a vector of elements in $\mathfrak{U}$ such that for all i, j:
- $b_i = b_j$ iff $a_i = a_j$,
- if $a_i \in \mathfrak{U}$ then $a_i = b_i$, and
- if $a_i \notin \mathfrak{U}$ then $b_i \in \left\{\mathfrak{s}(c_j) \mid j \in [1, m]\right\}$.

It is straightforward to verify that such a sequence always exists. Furthermore, by definition of φ_∞, $c_i^{\mathfrak{i}}$ does not occur in $\mathfrak{p}^{\mathfrak{i}}$, hence $(\mathfrak{U}, \mathfrak{s}[y_1 \leftarrow b_1] \ldots [y_m \leftarrow b_m], \mathfrak{i})$ and $(\mathfrak{U}', \mathfrak{s}[y_1 \leftarrow a_1] \ldots [y_m \leftarrow a_m], \mathfrak{i})$ coincide on every atom in ϕ. Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \varphi$ we deduce that $(\mathfrak{U}, \mathfrak{s}[y_1 \leftarrow b_1] \ldots [y_m \leftarrow b_m], \mathfrak{i}) \models \phi$, hence $(\mathfrak{U}', \mathfrak{s}[y_1 \leftarrow a_1] \ldots [y_m \leftarrow a_m], \mathfrak{i}) \models \phi$. Since $\mathbf{a}$ is arbitrary, we deduce that $(\mathfrak{U}', \mathfrak{s}, \mathfrak{i}) \models \varphi$. The converse is immediate. □

The first decidability result of this paper is stated below:

Theorem 2. *For any integer $k \geq 1$ not depending on the input, the infinite satisfiability problem for $\mathsf{BSR}^{inf}(\mathsf{SL}^k)$ is PSPACE-complete.*

Proof PSPACE-hardness is an immediate consequence of the fact that the quantifier-free fragment of SL^k, without the separating implication, but with the separating conjunction and negation, is PSPACE-hard [6, Proposition 5].

To show membership in PSPACE, let $\varphi = \forall y_1 \ldots \forall y_m \,.\, \phi$ be a sentence in $\mathsf{BSR}^{inf}(\mathsf{SL}^k)$, where ϕ is quantifier-free and $\mathsf{var}(\phi) = \{x_1, \ldots, x_n, y_1, \ldots, y_m\}$. Let $\varphi' \stackrel{\text{def}}{=} \forall y_1 \ldots \forall y_m \,.\, \bigvee_{M \in \mu^{inf}(\phi)} M$. If $\mathsf{alloc}(x)$ occurs in a minterm in $\mu^{inf}(\phi)$, then by Lemma 6, x necessarily occurs in the scope of a positive occurrence of $\twoheadrightarrow$, which entails by definition of $\mathsf{BSR}^{inf}(\mathsf{SL}^k)$ that $x \notin \{y_1, \ldots, y_n\}$. Therefore, by Lemma 2, there exists a $\mathsf{BSR}(\mathsf{FO})$ formula equivalent to $\tau(\varphi')$, with the same constants and free variables as $\tau(\varphi')$. Consequently, the same holds for the formula $\psi \stackrel{\text{def}}{=} \tau(\varphi') \wedge \mathcal{A}(\varphi')$ (Definition 4). Let ψ_∞ be the formula defined in Definition 9. By definition, ψ_∞ is in $\mathsf{BSR}(\mathsf{FO})$ and contains exactly m constants not occurring in ψ. Thus $\psi \wedge \psi_\infty$ has a model iff it has a model $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$, with $||\mathfrak{U}|| \leq \max(1, p + m + n)$, where p denotes the number of constants and free variables in $\mathcal{A}(\varphi')$ [2, Proposition 6.2.17]. We have $p = \mathcal{O}(\mathcal{N}(\varphi'))$ and, by Corollary 1, $p = \mathcal{O}(\mathsf{size}(\varphi)^2)$, so that $||\mathfrak{U}|| = \mathcal{O}(\mathsf{size}(\varphi)^2)$. Then we can guess a FO-structure $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$ such that $||\mathfrak{U}|| = \mathcal{O}(\mathsf{size}(\varphi)^2)$ and check that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\varphi') \wedge \mathcal{A}(\varphi') \wedge \psi_\infty$. This test is feasible in PSPACE:

- the problem $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\varphi')$ is in PSPACE by Lemma 2,
- the problem $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \mathcal{A}(\varphi')$ is in P, because $\mathcal{A}(\varphi')$ is a conjunction of $\mathcal{O}(p)$ universally quantified formulae, each having a constant number of universal quantifiers, because k does not depend on the input, and
- the problem $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \psi_\infty$ is also in P, since it suffices to check that the $c_1^{\mathfrak{i}}, \ldots, c_m^{\mathfrak{i}}$ are pairwise distinct, distinct from $\mathfrak{s}(x_1), \ldots, \mathfrak{s}(x_n)$ and, moreover, do not occur in $\mathfrak{p}^{\mathfrak{i}}$.

Finally, by Proposition 21, $\psi \wedge \psi_\infty$ is satisfiable iff ψ admits an infinite model for which $||\mathfrak{p}^{\mathfrak{i}}|| \in \mathbb{N}$. By Lemma 1, the latter property holds iff φ has an infinite model. □

In the remainder, we prove that finite satisfiability is PSPACE-complete for the class $\mathsf{BSR}^{fin}(\mathsf{SL}^k)$, defined as the set of formulae with no positive occurrence of separating implications. Even with this stronger restriction, the previous proof based on a translation to first-order logic requires an additional argument. The problem is that, in the case of a finite universe, $\mathsf{alloc}(x)$ test formulae may occur at a positive polarity, even if every $\phi_1 \twoheadrightarrow \phi_2$ subformula occurs at a negative polarity, due to the positive occurrences of $\mathsf{alloc}(x)$ within λ^{fin} (14) in the definition of $\mathsf{elim}^{fin}_{\multimap}(M_1, M_2)$, used for the elimination of separating implications. As previously discussed (Remark 1), positive occurrences of $\mathsf{alloc}(x)$ hinder the translation into $\mathsf{BSR}(\mathsf{FO})$, because of the existential quantifiers that may occur in the scope of a universal quantifier.

The solution is to distinguish a class of finite structures $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$, so-called *$\alpha$-controlled structures*, for some $\alpha \in \mathbb{N}$, for which there exists a set of locations $\ell_1, \ldots, \ell_\alpha$, such that every location $\ell \in \mathfrak{U}$ is either ℓ_i or points to a tuple from the set $\{\ell_1, \ldots, \ell_\alpha, \ell\}$. An example of a 3-controlled structure is given in Figure 2.

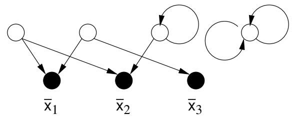

Fig. 2. A finite 3-controlled SL^2 structure.

Definition 10. *A structure $\mathcal{I}$ is α-controlled iff $\mathcal{I} \models C(\alpha)$, where*

$$C(\alpha) \stackrel{\mathsf{def}}{=} \exists \overline{\mathsf{x}}_1 \ldots \exists \overline{\mathsf{x}}_n \forall x \, . \, \bigvee_{i=1}^{\alpha} x \approx \overline{\mathsf{x}}_i \vee \bigvee_{\mathbf{y} \in \mathsf{vect}^k(\overline{\mathsf{x}}_1, \ldots, \overline{\mathsf{x}}_\alpha, x)} x \hookrightarrow \mathbf{y}$$

and $\mathsf{vect}^k(S)$ is the set of k-tuples of symbols in S.

Note that any α-controlled structure is finite, since $\mathfrak{U} = \mathrm{dom}(\mathfrak{h}) \cup \{\mathfrak{s}(\overline{\mathsf{x}}_1), \ldots, \mathfrak{s}(\overline{\mathsf{x}}_\alpha)\}$, but its cardinality is not necessarily bounded. Furthermore, if $||\mathfrak{U}|| \leq \alpha$, then $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ is necessarily α-controlled, since we can extend $\mathfrak{s}$ to a store $\mathfrak{s}'$ such that $\mathfrak{U} \subseteq \{\mathfrak{s}'(\overline{\mathsf{x}}_1), \ldots, \mathfrak{s}'(\overline{\mathsf{x}}_\alpha)\}$.

For a sentence $\varphi = \forall y_1 \ldots \forall y_m \, . \, \phi$ in $\mathsf{BSR}^{fin}(\mathsf{SL}^k)$, we distinguish the following cases:

1. If φ has an α-controlled model $\mathcal{I}$, the formula obtained by replacing each occurrence of an $\mathsf{alloc}(x)$ with $\bigwedge_{i=1}^{\alpha}(x \approx \overline{\mathsf{x}}_i \rightarrow \mathsf{alloc}(\overline{\mathsf{x}}_i))$ in $\forall y_1 \ldots \forall y_m$ $\bigvee_{M \in \mu^{fin}(\phi)} M$ is satisfied by $\mathcal{I}$,[12]
2. Otherwise, each finite model of φ is non-α-controlled and we can build a model $\mathcal{I}$, with a sufficiently large universe, such that each test formula $\theta \in \{|U| \geq n, |h| < |U| - n \mid n \in \mathbb{N}\}$ becomes true in $\mathcal{I}$. Because each positive occurrence of $\mathsf{alloc}(x)$ in a λ^{fin} (14) subformula of some $\mathsf{elim}^{fin}_{-\!\!\circledast}(M_1, M_2)$ formula generated by the elimination of the separating implication from ϕ occurs in disjunction with a formula $|h| < |U| - n_1 \wedge |U| \geq n_2$, which is satisfied by $\mathcal{I}$, its truth value in $\mathcal{I}$ can be ignored.

In both cases, we obtain an equisatisfiable universally quantified boolean combination of test formulae with no positive occurrence of $\mathsf{alloc}(y_i)$ formulae, for any universally quantified variable y_i. We translate this into an equisatisfiable $\mathsf{BSR}(\mathsf{FO})$ sentence, for which finite satisfiability is decidable and apply a similar argument to that for the infinite case, to obtain the PSPACE upper bound.

Lemma 9. *Given a formula $\varphi \in \mathsf{BSR}^{fin}(\mathsf{SL}^k)$ and a number $\alpha \in \mathbb{N}$ encoded in unary, the problem whether φ has an α-controlled model is in PSPACE.*

Proof: Let $x_1, \ldots, x_n$ be the existentially quantified variables occurring in φ and let φ' be the prenex form of $\varphi \wedge C(\alpha)$. It is clear that φ' is of the form

[12] If $\mathcal{I}$ is α-controlled, then $\mathcal{I} \models \mathsf{alloc}(x) \leftrightarrow \bigwedge_{i=1}^{\alpha}(x \approx \overline{\mathsf{x}}_i \rightarrow \mathsf{alloc}(\overline{\mathsf{x}}_i))$.

$\forall y_1 \ldots \forall y_m \,.\, \phi$, where ϕ is quantifier-free. Moreover, by definition, φ has an α-controlled model iff φ' has a model, and this model is necessarily finite.

We denote by $\gamma(\phi)$ the formula obtained from $\bigvee_{M \in \mu^{fin}(\phi)} M$ by replacing every formula $\mathsf{alloc}(x)$ with $\bigwedge_{i=1}^{\alpha}(x \approx \overline{\mathsf{x}}_i \rightarrow \mathsf{alloc}(\overline{\mathsf{x}}_i))$. Let $\psi \stackrel{\mathsf{def}}{=} \forall y_1 \ldots \forall y_m \,.\, \gamma(\phi)$ and $\psi' \stackrel{\mathsf{def}}{=} \forall y_1 \ldots \forall y_m \,.\, \bigvee_{M \in \mu^{fin}(\phi)} M$. We have $\psi \equiv \psi'$ because, in each structure $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models C(\alpha)$, all locations must be allocated, except possibly for $\mathfrak{s}(\overline{\mathsf{x}}_1), \ldots, \mathfrak{s}(\overline{\mathsf{x}}_\alpha)$, thus $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \mathsf{alloc}(x) \leftrightarrow \bigwedge_{i=1}^{\alpha}(x \approx \overline{\mathsf{x}}_i \rightarrow \mathsf{alloc}(\overline{\mathsf{x}}_i))$.

The formula ψ contains no occurrence of $\mathsf{alloc}(y_i)$, since by definition the only test formulae $\mathsf{alloc}(x)$ occurring in $\gamma(\phi)$ are such that $x \in \{\overline{\mathsf{x}}_1, \ldots, \overline{\mathsf{x}}_\alpha\}$. Thus, by Lemma 2, $\tau(\psi)$ is equivalent to a formula in $\mathsf{BSR}(\mathsf{FO})$ with the same free variables and constants. Therefore, the same holds for $\tau(\psi) \wedge \mathcal{A}(\psi)$, and $\tau(\psi) \wedge \mathcal{A}(\psi)$ has a model iff it has a model $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$, with $||\mathfrak{U}|| = n + \alpha + \mathcal{O}(\mathcal{N}(\gamma(\phi)))$, since $\tau(\psi)$ contains $n+\alpha$ free variables and some constants from $\mathcal{A}(\psi)$, and the number of constants and free variables in $\mathcal{A}(\psi)$ is bounded by $\mathcal{O}(\mathcal{N}(\gamma(\phi)))$. We have $\mathcal{N}(\gamma(\phi)) = \mathcal{N}(\psi')$, thus by Corollary 1, $\mathcal{N}(\gamma(\phi))$ is bounded by $\mathcal{O}(\mathsf{size}(\varphi')^2)$, and $||\mathfrak{U}|| = \mathcal{O}(\mathsf{size}(\varphi')^2) = \mathcal{O}((\mathsf{size}(\varphi) + \alpha)^2)$.

Therefore $\tau(\psi) \wedge \mathcal{A}(\psi)$ has a model iff it has a model $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$, with $||\mathfrak{U}|| = \mathcal{O}((\mathsf{size}(\varphi)+\alpha)^2)$. Then we can guess a structure $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$ such that $||\mathfrak{U}|| = \mathcal{O}((\mathsf{size}(\varphi)+\alpha)^2)$ and check in polynomial space whether $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\psi)$, by Corollary 2, and whether $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \mathcal{A}(\psi)$, as it is done in the proof of Theorem 2. By Lemma 1, $\tau(\psi) \wedge \mathcal{A}(\psi)$ has a model iff ψ has a finite model. Since $\psi \equiv \psi'$ we deduce by Lemma 5 that $\tau(\psi) \wedge \mathcal{A}(\psi)$ has a finite model iff φ' has a finite model iff φ has an α-controlled model. □

Lemma 10. *Let $m \geq 1$ be an integer and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ be a finite non-α-controlled structure, where $\alpha > (k+1) \times (||\mathfrak{D}|| + m)$ for a set $\mathfrak{D} \subseteq \mathfrak{U}$. Then for any universe $\mathfrak{U}' \supseteq \mathfrak{U}$ and each tuple $(a_1, \ldots, a_m) \in (\mathfrak{U}')^m$ there exists a tuple $(b_1, \ldots, b_m) \in \mathfrak{U}^m$ such that, for all $i, i' \in [1, m]$:*

1. *if $a_i \in \mathfrak{U}$ then $b_i = a_i$,*
2. *$b_i = b_{i'}$ iff $a_i = a_{i'}$,*
3. *if $a_i \notin \mathfrak{U}$ then for no $\ell \in \mathfrak{D} \cap \mathrm{dom}(\mathfrak{h})$ does b_i occur in $\mathfrak{h}(\ell)$,*
4. *if $a_i \notin \mathfrak{U}$ then $\mathfrak{h}(b_i)$ is either undefined or contains a location that does not occur in $\{b_1, \ldots, b_m\} \cup \mathfrak{D}$.*

Proof: Let $X \stackrel{\mathsf{def}}{=} \left\{p \in [1, m] \mid a_p \in \mathfrak{U}\right\}$ and $X' \stackrel{\mathsf{def}}{=} \{j_1, \ldots, j_{m'}\} \stackrel{\mathsf{def}}{=} [1, m] \setminus X$. For all $p \in X$, we set $b_p \stackrel{\mathsf{def}}{=} a_p$. The sequence b_{j_i} for $1 \leq i \leq m'$ is constructed inductively as follows. Assume that $b_{j_1}, \ldots, b_{j_i}$ is constructed. If $a_{j_{i+1}} = a_{j_p}$, for some $p \in [1, i]$ then we set $b_{j_{i+1}} \stackrel{\mathsf{def}}{=} b_{j_p}$. Otherwise, we define the sets S_i and S'_i

as follows:

$$S_i \stackrel{\text{def}}{=} \{b_p \mid p \in X\} \cup \{b_{j_1}, \ldots, b_{j_i}\} \cup \mathfrak{D}$$
$$S'_i \stackrel{\text{def}}{=} \{\ell_1, \ldots, \ell_k \mid \ell \in \mathrm{dom}(\mathfrak{h}) \cap S_i \text{ and } \mathfrak{h}(\ell) = (\ell_1, \ldots, \ell_k)\}.$$

By definition, $T \stackrel{\text{def}}{=} S_i \cup S'_i$ contains less than $(k+1) \times (n+m)$ elements: indeed, there are at most $n+m$ elements in S_i, and for each element ℓ in S_i, there are at most k elements in $\mathfrak{h}(\ell)$. By hypothesis, $(k+1) \times (n+m) < \alpha$. Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$ is non-α-controlled, this means that there exists a location $\ell \in \mathfrak{U} \setminus T$, such that $\mathfrak{h}(\ell)$ is either undefined or contains a location not occurring in $T \cup \{\ell\}$. We then let $b_{j_{i+1}} \stackrel{\text{def}}{=} \ell$.

Conditions 1-3 are a straightforward check. We prove that condition 4 also holds, by contradiction. Suppose that $a_{j_i} \notin \mathfrak{U}$ and $b_{j_i} \in \mathrm{dom}(\mathfrak{h})$, where $\mathfrak{h}(b_{j_i}) = (\ell_1, \ldots, \ell_k)$ and $\{\ell_1, \ldots, \ell_k\} \subseteq \{b_1, \ldots, b_m\} \cup \mathfrak{D}$. By construction of b_{j_i}, $\mathfrak{h}(b_{j_i})$ contains an element, say ℓ_s, for some $s \in [1, k]$, that does not belong to $S_{i-1} \cup S'_{i-1} \cup \{b_{j_i}\}$. Since $S_{i-1} = \{b_p \mid p \in X\} \cup \{b_{j_1}, \ldots, b_{j_{i-1}}\} \cup \mathfrak{D}$, necessarily, $\ell_s = b_{j_{i'}}$ for some $i < i' \leq m'$, because $\ell_s \in \{b_1, \ldots, b_m\} \cup \mathfrak{D}$ by hypothesis. However, $b_{j_i} \in S_{i'-1}$, because $i < i'$, and therefore $\ell_s \in S'_{i'-1}$, and we cannot have $b_{j_{i'}} = \ell_s$, contradiction. □

We state below the second decidability result of the paper, concerning the decidability of the finite satisfiability for $\mathsf{BSR}^{fin}(\mathsf{SL}^k)$:

Theorem 3. *For any integer $k \geq 1$, not depending on the input, the finite satisfiability problem for $\mathsf{BSR}^{fin}(\mathsf{SL}^k)$ is PSPACE-complete.*

Proof PSPACE-hardness is proved using the same argument as in the proof of Theorem 2, which does not rely on the finiteness of the universe.

Let $\varphi = \forall y_1, \ldots, y_m . \phi$ be a sentence in $\mathsf{BSR}^{fin}(\mathsf{SL}^k)$, where ϕ is quantifier-free and $\mathsf{var}(\phi) = \{x_1, \ldots, x_n, y_1, \ldots, y_m\}$. Let $\alpha \stackrel{\text{def}}{=} (\max((k+1) \times (n+m), \beta) + 1$, with $\beta \stackrel{\text{def}}{=} \mathcal{N}(\bigvee_{M \in \mu^{fin}(\phi)} M)$. We first check whether φ admits an α-controlled model, which can be done in PSPACE, by Lemma 9 since $\beta = \mathcal{O}(\mathsf{size}(\varphi)^2)$, thus $\alpha = \mathcal{O}(\mathsf{size}(\varphi)^2)$. In this case, φ has a finite model, and otherwise φ has a finite model iff it has a non-α-controlled finite model. We now assume that φ does not have an α-controlled model.

Let $\varphi' \stackrel{\text{def}}{=} \forall y_1, \ldots, y_m . \delta(\phi)$, where $\delta(\phi)$ is obtained by replacing all positive occurrences of $\mathsf{alloc}(x)$, with $x \in \{x_1, \ldots, x_n, y_1, \ldots, y_m\}$, by $\bot$, in $\bigvee_{M \in \mu^{fin}(\phi)} M$. We shall prove that φ' has a finite model iff φ has a finite non-α-controlled model. By Lemma 5, φ has a finite model iff $\forall y_1, \ldots, y_m . \bigvee_{M \in \mu^{fin}(\phi)} M$ has a finite model. Because the replaced occurrences of $\mathsf{alloc}(x)$ are all positive, it is clear that $\varphi' \models \forall y_1, \ldots, y_m . \bigvee_{M \in \mu^{fin}(\phi)} M$, thus the direct implication holds. Now, assume that $\forall y_1, \ldots, y_m \,.\, \bigvee_{M \in \mu^{fin}(\phi)} M$ admits a non-α-controlled finite model $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h})$. In particular, we have $||\mathfrak{U}|| > \alpha$.

We build a structure $(\mathfrak{U}', \mathfrak{s}, \mathfrak{h})$, where $\mathfrak{U}'$ is obtained by adding $\max(0, ||\mathfrak{h}|| + \beta - ||\mathfrak{U}|| + 1)$ fresh locations to $\mathfrak{U}$, so that $||\mathfrak{U}'|| > ||\mathfrak{h}|| + \beta$. Let $\mathbf{a} = (a_1, \ldots, a_m) \in (\mathfrak{U}')^m$ be an arbitrary tuple of locations. We show that $(\mathfrak{U}', \mathfrak{s}[y_i \leftarrow a_i \mid i = 1, \ldots, n], \mathfrak{h}) \models \delta(\phi)$. By Lemma 10, taking $\mathfrak{D} = \{\mathfrak{s}(x_i) \mid i \in [1, n]\} \subseteq \mathfrak{U}$, there exists a tuple $\mathbf{b} = (b_1, \ldots, b_m) \in \mathfrak{U}^m$ satisying the conditions (1), (2), (3) and (4) of Lemma 10. Let $\mathfrak{s}_a \stackrel{\text{def}}{=} \mathfrak{s}[y_i \leftarrow a_i \mid i = 1, \ldots, m]$ and $\mathfrak{s}_b \stackrel{\text{def}}{=} \mathfrak{s}[y_i \leftarrow b_i \mid i = 1, \ldots, m]$. Since $(\mathfrak{U}, \mathfrak{s}, \mathfrak{h}) \models \forall y_1 \ldots \forall y_m \,.\, \bigvee_{M \in \mu^{fin}(\phi)} M$, we have $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \models \bigvee_{M \in \mu^{fin}(\phi)} M$, hence there exists a minterm $M \in \mu^{fin}(\phi)$ such that $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \models M$. We show that for all literals ℓ occurring in M: $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \models \ell \Rightarrow (\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models \ell$, by distinguishing the following cases:

$\ell \in \{x \approx y, \neg x \approx y\}$. By conditions (1) and (2) of Lemma 10, $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h})$ and $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h})$ coincide on every equational atom $x \approx y$.

$\ell \in \{t_0 \hookrightarrow (t_1, \ldots, t_k), \neg t_0 \hookrightarrow (t_1, \ldots, t_k)\}$. We show that $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \models t_0 \hookrightarrow (t_1, \ldots, t_k)$ iff $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models t_0 \hookrightarrow (t_1, \ldots, t_k)$. Note that we have $t_0, \ldots, t_k \in \{x_1, \ldots, x_n, y_1, \ldots, y_m\}$. Let $Y \stackrel{\text{def}}{=} \{i \in [1, m] \mid y_i \in \{t_0, \ldots, t_k\}\}$. We distinguish several cases:

1. $\{a_i \mid i \in Y\} \subseteq \mathfrak{U}$. In this case, for all $j \in [0, k]$, we have $\mathfrak{s}_b(t_j) = \mathfrak{s}_a(t_j)$. This is immediate when $t_j \in \{x_1, \ldots, x_n\}$, and when $t_j = y_{j'}$ for some $j' \in Y$, this is due to the fact that $b_{j'} = a_{j'}$ by condition (1) of Lemma 10. Consequently, $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \models t_0 \hookrightarrow (t_1, \ldots, t_k)$ iff $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models t_0 \hookrightarrow (t_1, \ldots, t_k)$.
2. There is an $i \in Y$ such that $a_i \notin \mathfrak{U}$. Then $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \not\models t_0 \hookrightarrow (t_1, \ldots, t_k)$, since $a_i \notin \mathfrak{U}$. We show that $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \not\models t_0 \hookrightarrow (t_1, \ldots, t_k)$ by distinguishing the following cases:
   (a) $t_0 = y_i$. By condition (4) of Lemma 10, either $\mathfrak{h}(b_i)$ is undefined or it contains an element that does not occur in $\{b_1, \ldots, b_m\} \cup D$. In the first case, $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \not\models t_0 \hookrightarrow (t_1, \ldots, t_k)$. In the second case, assuming that $\mathfrak{h}(b_i) = (\ell_1, \ldots, \ell_k)$, there is an $s \in [1, k]$ such that $\ell_s \notin \{b_1, \ldots, b_m\} \cup \mathfrak{D}$. Since $\mathfrak{s}_b(t_s) \in \{b_1, \ldots, b_m\} \cup \mathfrak{D}$, we obtain $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \not\models t_0 \hookrightarrow (t_1, \ldots, t_k)$.
   (b) $t_0 \in \{x_1, \ldots, x_n\}$ and $t_s = y_i$ for some $s \in [1, k]$. By condition (3) of Lemma 10, b_i does not occur in the tuple $\mathfrak{h}(\ell)$ for any $\ell \in \mathfrak{D} \cap \mathrm{dom}(\mathfrak{h})$. Consequently, $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \not\models t_0 \hookrightarrow (t_1, \ldots, t_k)$.
   (c) $t_0 = y_j$ with $a_j = b_j \in \mathfrak{U}$ and $t_s = y_i$ for some $s \in [1, k]$. Then, by condition (3) of Lemma 10, b_i is not an element of $\mathfrak{h}(b_j)$, thus $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h}) \not\models t_0 \hookrightarrow (t_1, \ldots, t_k)$.

$\ell \in \{|h| \geq |U| - i \mid i \in \mathbb{N}\}$. This case is impossible, because φ contains no positive occurrence of $-\!\!\circledast$ and by Lemma 6, $\bigvee_{M \in \mu^{fin}(\phi)} M$ contains no positive literal $|h| \geq |U| - i$.

$\ell \in \{|U| \geq i, |h| < |U| - i \mid i \in \mathbb{N}\}$. We obtain $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models \ell$, because $||\mathfrak{U}'|| > \beta \geq i$ by definition of β.

$\ell \in \{|U| < i \mid i \in \mathbb{N}\}$. These formulae are false in $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h})$, since $||\mathfrak{U}|| > \alpha > \beta \geq i$ by definition of β.

$\ell = \neg\mathsf{alloc}(x)$. If $\mathfrak{s}_a(x) \in \mathfrak{U}$ then $(\mathfrak{U}, \mathfrak{s}_b, \mathfrak{h})$ and $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h})$ coincide on $\mathsf{alloc}(x)$. Otherwise, $\mathfrak{s}_a(x) \notin \mathrm{dom}(\mathfrak{h})$ and $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models \neg\mathsf{alloc}(x)$.

Consequently, if M contains no literal of the form $\mathsf{alloc}(x)$ then $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models M$, hence $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models \delta(\phi)$. Otherwise, let $\{\mathsf{alloc}(x_1), \ldots, \mathsf{alloc}(x_p)\}$ be the set of literals $\mathsf{alloc}(x)$ occurring in M. Since all occurrences of $\twoheadrightarrow$ in φ are negative or neutral, by Lemma 6 (point 4), every literal $\mathsf{alloc}(x_i)$ occurs within a subformula λ^{fin} of some formula $\mathsf{elim}^{fin}_{\multimap}(M_1, M_2)$, hence inside a formula of the form $\mathsf{alloc}(x_i) \vee (|h| < |U| - q_i \wedge |U| \geq r_i)$, for some $q_i, r_j \leq \beta$. Thus $\mu^{fin}(\phi)$ necessarily contains a minterm M' identical to M, except that each literal $\mathsf{alloc}(x_i)$ is replaced by $(|h| < |U| - q_i \wedge |U| \geq r_i)$. But, by definition, $\mathfrak{U}'$ contains more than β unallocated elements, hence necessarily $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models (|h| < |U| - q_i \wedge |U| \geq r_j)$. Therefore, $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models M' \models \delta(\phi)$.

We have proved that $(\mathfrak{U}', \mathfrak{s}_a, \mathfrak{h}) \models \delta(\phi)$. Since **a** is arbitrary, we deduce that $(\mathfrak{U}', \mathfrak{s}, \mathfrak{h}) \models \forall y_1, \ldots, y_m \,.\, \delta(\phi) = \varphi'$.

Consequently, it is sufficient to test that φ' has a finite model. We show that the finite satisfiability problem for φ' is in PSPACE. By Lemma 2, since by definition $\delta(\phi)$ contains no positive occurrence of $\mathsf{alloc}(x)$, the formula $\tau(\varphi') \wedge \mathcal{A}(\varphi')$ is equivalent to a formula in BSR(FO) with the same free variables and constants, and $\tau(\varphi') \wedge \mathcal{A}(\varphi')$ has a finite model iff it has a model $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$, with $||\mathfrak{U}|| = n + O(\mathcal{N}(\delta(\phi)))$, since the number of constants and free variables in $\tau(\varphi') \wedge \mathcal{A}(\varphi')$ is $n + O(\mathcal{N}(\delta(\phi)))$. It is clear that $\mathcal{N}(\delta(\phi)) = \mathcal{N}(\bigvee_{M \in \mu^{fin}(\phi)} M)$, hence by Corollary 1, $\mathcal{N}(\delta(\phi)) = O(\mathsf{size}(\varphi)^2)$, thus $||\mathfrak{U}|| = O(\mathsf{size}(\varphi)^2)$.

Then we can guess a FO-structure $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i})$ such that $||\mathfrak{U}|| = O(\mathsf{size}(\varphi)^2)$ and check in polynomial space that $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \tau(\varphi')$ (this is done as in Lemma 2, except that the minterms containing a test formula $\mathsf{alloc}(x)$ are discarded) and $(\mathfrak{U}, \mathfrak{s}, \mathfrak{i}) \models \mathcal{A}(\varphi')$ (as in the proof of Theorem 2). By Lemma 1, the formula $\tau(\varphi') \wedge \mathcal{A}(\varphi')$ has a finite model iff φ' has a finite model, i.e., iff φ has an non-α-controlled finite model (since we know at this point that φ has no finite α-controlled model). □

Note that the PSPACE-completeness results for $\mathsf{BSR}^{fin}(\mathsf{SL}^k)$ and $\mathsf{BSR}^{inf}(\mathsf{SL}^k)$ allow us to re-establish the PSPACE-completeness of the satisfiability problem for quantifier-free formulae of SL^k, both in finite and infinite domains. Indeed, every quantifier-free formula ϕ is sat-equivalent to a formula $\phi \multimap \top$ that is both in $\mathsf{BSR}^{fin}(\mathsf{SL}^k)$ and $\mathsf{BSR}^{inf}(\mathsf{SL}^k)$, since the antecedent of $\twoheadrightarrow$ has neutral polarity.

6 Conclusions and Future Work

We have studied the decidability problem for the class of Separation Logic formulae with quantifier prefix in the language $\exists^*\forall^*$, denoted as $\mathsf{BSR}(\mathsf{SL}^k)$. Although the fragment was found to be undecidable, we identified two non-trivial subfragments for which the infinite and finite satisfiability are PSPACE-complete. These fragments are defined by restricting the use of universally quantified variables within the scope of separating implications that occur at positive polarity. Since, in practice, solving most Separation Logic entailments that arise as verification conditions in programs or inductive solvers do not involve considering separating implications that contain universally quantified variables, the decidable classes found in this work are of practical interest.

Future work involves using the techniques for proving decidability, namely the translation of quantifier-free SL^k formulae into boolean combinations of test formulae, to solve other logical problems, such as frame inference, abduction and possibly interpolation.

Acknowledgements The authors wish to acknowledge the contributions of Stéphane Demri and Étienne Lozes to the insightful discussions during the early stages of this work. ■

References

1. S. Arora and B. Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009.
2. E. Börger, E. Grädel, and Y. Gurevich. *The Classical Decision Problem*. Perspectives in Mathematical Logic. Springer, 1997.
3. R. Brochenin, S. Demri, and E. Lozes. On the almighty wand. *Information and Computation*, 211:106 – 137, 2012.
4. C. Calcagno and D. Distefano. Infer: An automatic program verifier for memory safety of c programs. In *Proc. of NASA Formal Methods'11*, volume 6617 of *LNCS*. Springer, 2011.
5. C. Calcagno, P. Gardner, and M. Hague. From separation logic to first-order logic. In *FOSSACS*, pages 395–409. Springer, 2005.
6. C. Calcagno, H. Yang, and P. W. O'Hearn. Computability and complexity results for a spatial assertion language for data structures. In *FST TCS 2001, Proceedings*, pages 108–119. Springer, 2001.
7. S. Demri and M. Deters. Expressive completeness of separation logic with two variables and no separating conjunction. *ACM Trans. Comput. Logic*, 17(2):1–44, Jan. 2016.
8. S. Demri, D. Galmiche, D. Larchey-Wendling, and D. Méry. Separation logic with one quantified variable. In *CSR'14*, volume 8476 of *LNCS*, pages 125–138. Springer, 2014.
9. S. S. Ishtiaq and P. W. O'Hearn. Bi as an assertion language for mutable data structures. In *ACM SIGPLAN Notices*, volume 36, pages 14–26, 2001.
10. E. Lozes. Separation logic preserves the expressive power of classical logic. In *SPACE*, 2004.

11. F. P. Ramsey. On a problem of formal logic. *Classic Papers in Combinatorics*, pages 1–24, 1987.
12. A. Reynolds, R. Iosif, and C. Serban. Reasoning in the bernays-schönfinkel-ramsey fragment of separation logic. In *VMCAI*, pages 462–482. Springer, 2017.
13. A. Reynolds, R. Iosif, C. Serban, and T. King. A decision procedure for separation logic in SMT. In *ATVA*, pages 244–261, 2016.
14. J. Reynolds. Separation Logic: A Logic for Shared Mutable Data Structures. In *Proc. of LICS'02*, 2002.
15. W. J. Savitch. Relationships between nondeterministic and deterministic tape complexities. *Journal of Computer and System Sciences*, 4(2):177 – 192, 1970.